From secure wired networks to secure wireless networks –

What are the extra risks?

Keywords : Information Security, Wireless Networks, WiFi Security

Prof Basie von Solms
Dr Emil Marais

RAU-Standard Bank Academy for Information Technology
RAU University
Johannesburg

1. Introduction

The purpose of this paper is to give a high level overview of the risks involved in inmplementing wireless networks, and some suggestions on how such risks can be controlled and mediated.

No real technical aspects will be addressed in the paper.

To investigate the essentials of secure wireless networks, we must first investigate the essentials of secure wired networks.

The reason for this approach is because ' a secure wireless network is dependant on a secure wired network.'

We will therefore start off in paragraph 2 by briefly reviewing the essentials of a secure wired network.

In paragraph 3 we will apply these essentials to wireless networks, and investigate what else, over and above those essentials for secure wired networks, are needed for secure wireless networks.

In paragraph 4 we will provide a some practical guidelines on how to secure a wireless network.

2. The essentials of secure wired networks

The general approach to Information Security Governance, strongly influenced by international best practices for information security management, specifies that the following practices are needed for enforcing the security of wired networks :

2.1 A proper risk analysis

To properly secure a wired network, it is essential to have a good understanding of what risks are relevant to the use of such a network. Therefore some sort of risk analaysis must be done to know what these risks are, and what counter measures are needed to mediate them.

2.2 A proper network security policy

Such a policy, which should flow from the company's Corporate Information Security policy, should address aspects like :

- who may have access
- what procedures must be followed to have access
- what types of information may be transmitted over what networks
- what encryption techniques are used to enforce the confidentiality of transmitted data and information
- under what circumstances may new workstations be added to the network

2.3 Control the perimeters of your network

One of the basics of a secure wired network is to know precisely all the access point to the network are, and then secure those access points thorough proper firewalling

2.4 Enforcing identification and authentication, confidentiality and integrity

Technologies to enforce identification and authentication, confidentiality and integrity for data and information must be implemented, and enforced.

2.5 Implement proper compliance monitoring mechanisms

It is no use having a policy if the policy is not enforced and complied with.

Any wired network should be supplemented by the facility to monitor and enforce compliance to the relevant policies.

From the assumption that a secure wireless network depends on a secure wired network, it is clear that everything discussed in this paragraph are essential for a secure wireless network.
All these essentials also hold for wireless networks, but other specific risks do arise in the use of wireless networks, which are not necessarily directly relevant to wired networks.
The next paragraph will investigate these extra risks.

3. What are the extra (new) risks (essentials) relevant to wireless networks?

In this paragraph we will discuss some of the aspects which complicate the security of wireless networks.

3.1 Wireless networks are easy to install

In contrast with installing a wired network, which needs significant knowledge, hardware, money and time, a wireless network access point is cheap, and can be installed very easily without much technical knowledge. The access point is just plugged into the wired network. This means that rogue (unauthorized) access points can be installed very easy, without proper authorization and configuration, and in that way become a potential unauthorized point into the wired network.

Because of this ease of implementation of wireless networks, very often no proper risk analysis is done before any wireless facilities are installed, and such networks can create large risks to the corporate network.
Furthermore, very often the wireless access point is connected to the wired network behind the company firewall, which increases the risks significantly.

3.2 The perimeter of wired networks are difficult to determine and control

Because of the aspects discussed in 3.1 above, and the fact that wireless waves spill are not restricted to wires, the existence of wireless networks is easier to determine, and to compromise. Eavesdroppers who merely listen to the airwaves, can locate wireless networks, and determine if encryption is used or not.

3.3 Configuration of access points

When an access point is installed, it must be configured as far as its security settings are concerned. In most cases, wireless access points ship with minimal security configurations like default identification and authentication features, no encryption etc.
If these security configurations are not properly set after installation, the access point becomes a serious risk to the corporate network, as it can be used in all types of malicious attacks against the corporate network.

3.4 Access points to the corporate network

Every wireless access point becomes an access point to the network. This means that every company work station, able to access such a wireless access point, must have firewall capabilities to protect against external hacking via this work station.

3.5 Ad hoc (peer to peer) networks

Two workstations equipped with wireless networks cards (or laptops with built in wireless capabilities) can form a direct network between them without going through any wireless access point. This of course creates severe risks for the corporate network.

3.6 Policy issues

Because of the novelty of wireless networks, and because of the ease of implementation, many companies have not yet addressed wireless networks in their network security policies, even though such networks may already exist in unauthorized mode in the company.

Network security policies must address the wireless network issue directly – either by forbidding it totally, or providing strict rules on using it.

3.7 Jamming and denial of service

It is easier to create denial of service attacks against wireless networks, because the networks can simply be flooded with static noise which may cause the shut down of a network.

From the aspects discussed above, the biggest potential danger is the ease of installing and using a wireless access point, resulting in unauthorized access points, with the subsequent bigger risk to the company.

In the next paragraph we will suggest some guidelines for securing wireless networks, based on the discussion in this paragraph.

4. Practical guidelines for securing wireless networks

The following guidelines are not necessarily comprehensive, but address those aspects which had been identified in the previous paragraph, and which must be addressed right from the start.

4.1 **Create a Wireless Network Security Policy**, or include a section on Wireless Network Security in the existing Network Security Policy

This is the absolute starting point, and must be done by all companies.

If a company decides not to implement any wireless networks at all, add a statement to the Network Security Policy along the lines of :

'The installation of any type of wireless network in the company is strictly forbidden.'

If a company does allow the use of wireless networks, then the policy must forbid all unauthorized access points and ad hoc peer to peer networks, and supply a procedure which must be followed in applying and getting approval for the installation of any access point or peer to peer network.

Other aspects which can be specified in the policy are :

- Such access point are only operational during specific hours, for eg office hours
- The workstations and laptops which may get access to a specific access point, must be pre-registered at the access point (MAC addresses)
- A requirement that the installation of any wireless access point must be based on a proper risk analysis performed for that specific installation
- All installed access points, wireless cards and operating systems must be configured according to set company security standards

If any wireless networks were deployed before such a policy was adopted, all such networks must be audited and forced to comply with the requirements of the policy.

4.2 Securely configuring all access point before they become operational

The Information Security Department of the company should have an in depth knowledge of all the security settings of the specific type of access point and operating system used, and should configure those settings according to set standards.

Examples are :

- disable the broadcasting feature of an access point where the access point constantly broadcast its name (Service Set Identifier - SSID) looking for workstations who wants to connect to it
- change the default vendor-set SSID for all newly installed access points
- enforce MAC filtering, limiting the stations which can connect to the access point – of course only in those cases where roaming is not necessarily required
- only allow connection at high connection speeds

The default settings of for eg Windows XP is a security risk if they are not specifically changed to more secure settings.

4.3 Enforce identification and authentication, encryption and integrity

Even though encryption and authentication features for wireless networks are still developing, and the existing ones are not foolproof, that which is available should be activated and used.

Even though the encryption and authentication features of Wired Equivalency Policy (WEP) have been proved to be insecure, it is better to use it than to use no encryption or authentication at all.
For more mission critical data, stronger authentication and authentication must be implemented through products from specialized vendors.

4.4 Compliance enforcement

Mechanisms to enforce the relevant policy, and to check such compliance, are essential.

One of the most important of such compliance measures is to determine the presence of any unauthorized access points. This can be done in more than one way, of which the following two are the most common :

- physically walking the network area with scanners, detecting all signals on a regular basis, and establishing the presence, if any, of unauthorized access points
- monitoring the whole environment with remote sensors which would pick up all signals. From these results unauthorized access points can be identified.

Depending on the physical environment covered, the first option may not be practical, while the second option again will be more expensive as sensors must be placed at many points.

Whatever approach is taken, this form of compliance monitoring is crucial to the security of the company's wireless environment.

Wireless security experts recommend 24x7 monitoring of airwaves to discover unauthorized and rogue access points, and to identify vulnerabilities and risks as they appear.

Such monitoring should identify, amongst others :

- rogue and unauthorized access points
- unencrypted and unauthenticated traffic
- ad hoc peer to peer networks
- default or improper SSIDs
- default XP wireless settings
- off-hours traffic

This form of intrusion detection is complementary to the normal (non wireless) intrusion detection systems used in secure wired networks.

What is also important to realize, is that a wireless network can be compromised before the 'attack' reached the wired network. By that time, the attacker is seen by the wired intrusion detection system as friendly, and the attack may not be noticed.

Only a wireless focused intrusion detection system can protect your network from attacks in the airwaves before the traffic reached the wired network.

5. Summary

Wireless networks can be a significant tool in increasing business productivity, and should be considered by all companies.

However, as discussed above, wireless networks bring with it a totally new set of security risks which must be evaluated and countered.

Insecure wireless networks can cause very serious risks to companies, and before installing any such networks, all these risks must be identified, evaluated, and based on the results, the necessary counter measures must be installed to secure the network.

This paper tried to highlight some of these serious risks, and suggest ways to address them.

References

1. 5 Practical Steps to secure your wireless LAN, AirDefense White Paper, www.airdefense.net

2. 2. Wireless LANs : Risks and Defenses, AirDefense White Paper, www.airdefense.net

3. How to tighten loose security in wireless networks, Stephen Trilling, www.computerworld.com/securitytopics

4. How to build a secure WLAN, James Liu, www.comp uterworld.com/mobiletopics

5. Understanding the Layers of Wireless LAN Security and Management, AirDefense White Paper, www.airdefense.net