CLUSIF SUMMARIES

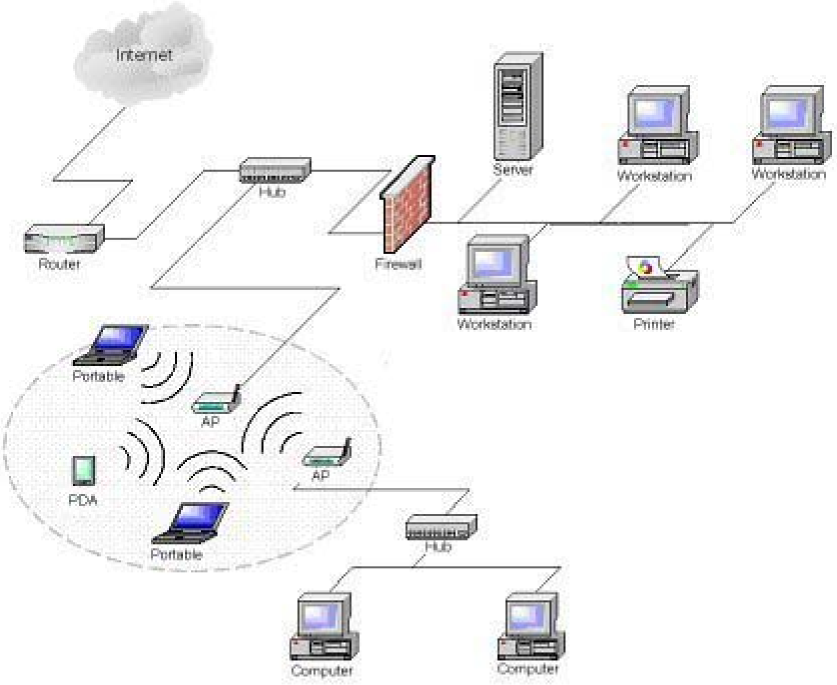
Wireless networks: threats, advantages and safeguards

1. Introduction

This document is designed to perform two functions: firstly to make companies and authorities aware of risks inherent to the deployment of a wireless network (WLAN) type 802.11b, and secondly to present solutions to improve security for this connection mode. This document does not deal with other standards such as 802.11a, 802.11i, 802.1x, Hiperlan, etc. or with personal infrastructures or hot spots.

2. Infrastructure

The type 802.11b WLAN is based on a standard (see references). It is a proximity radio transmission protocol on predetermined channels.



A typical structure combining ad hoc and Internet connection

The WLAN has some immediate advantages: ease of deployment, mobility of employees, interoperability of equipment, and low cost compared with the installation and maintenance of a wired network. It must be considered a priori as being a network open to the public but also **as a "risk bubble" in 3D**; a connection can be made from the street or from another floor or even from an aircraft (warflying, see references). Consequently, any uncontrolled connection can jeopardize the security of the entire information system.

The ease and low cost of implementation should be considered in parallel with essential improvements to the existing security configuration. This approach will be identical for any standard recent portable equipment that will be capable of connecting to a surrounding network or to other equipment by default, with the same resource (ad hoc connection).

3. Threats and impacts

Threat	Vector	Means	End purpose	Example
Interception	Connection and control flow	- Crypto analysis (crack, brute force) - Man in the Middle (MiM) - Masquerade / Replay - Message alteration	- CIA[1] attack on data in the I.S. - Attack on internal resources in the I.S. - Attack on resources in the I.S. connection	- Viewing data servers - Free internet
	Data flow	- Catching - Fake AP terminal (MiM) - Message corruption	- Disclosure - Fraudulent use	- Financial data from cash registers
Availability	Equipment	- Denial of Service - Interference by electromagnetic susceptibility	- Unavailability of WLAN - Resources transferred through the WLAN not available	- Video monitoring camera - Detection probes
War-Xing	- War driving - War driving and geopositioning (GPS) - War chalking[2]	- Proximity positioning	- Subsequent opportunity for interception or unavailability	- Network mapping on Internet - Floor marking
Ad hoc attacks	- Connection flow - Data flow	- ARP cache poisoning - Man in the Middle	- Generation of network packets losses - Malfunction of the machine	- Access to the wired network - Classical DoS attacks

[1] Confidentiality, Integrity, Availability

[2] Local marking (on the floor or on the walls)

Comments

The war-Xing is only a threat if the WLAN is not well secured.
Proximity detection and interception technologies are based on scanning software. Active scanners engage a dialog with the network: identification or connection requests. Passive scanners simply listen to different channels. This type of equipment is extremely portable, it may be a PDA or an innocent looking home made antenna.
All activity sectors are concerned by this exposure to risks. For example SMEs, due to their weak security means, financial institutions, the medical world and research and development due to the confidential and strategic nature of the data that they process.

4. Counter measures

These counter measures are necessary due to the weakness of the implemented protocol. At the present time, a firewall (DMZ) must be inserted between the WLAN and the existing local network.
It is illusory to try to systematically refuse this technology. If there is any pressure from users or management, it is better to control its deployment to prevent the development later on of "uncontrolled" installations (as was the case with "wild" modems when Internet first became available to the general public).
Note that AP cards and terminals are not suitable for installation in all industrial and medical environments, due to electromagnetic sensitivity or an excessively restrictive environment (heat, dust, etc.). Equipment for the general public is not sufficiently "hardened" and it would be very risky to deploy this type of resource on real time systems or in detection systems (fire safety). Furthermore, geographic coverage and / or interference problems may occur in the presence of materials that hinder propagation (concrete, steel mesh) or radiating equipment (machine tools, microwave ovens).
If a RADIUS or VPN architecture has already been set up, it will be possible to envisage deploying a wireless network without any large extra cost, while continuing to maintain security on the local network. In other cases, allowance will have to be made to set up security skills and for complementary investments at the beginning of the project, particularly for SMEs. One intermediate solution would consist of deploying a WLAN according to more recent standards only, for example 802.11i.

A) Equipment reconfiguration

Reconfiguration measures are usually inexpensive. They consist essentially of modifying equipment setup.

Architecture and topology

- There are two opposing architectures. Either each AP terminal is connected to the wired network, in which case constraints are exactly the same as constraints for a cabled network. Or all AP terminals are connected to each other and only one is connected to the network. In this case, authentication traffic will degrade throughput. Whatever solution is chosen, the connection with the wired network must be made through a firewall architecture.
- The physical arrangement of AP terminals has consequences. Whenever possible, antennas with directive radiation lobes should be chosen and APs should be placed in locations that reduce propagation outside the required volume, for example at a height or in the corner of a room. Thus, it is important to be vigilant about metallic infrastructures or ventilation ducts that act like wave guides and propagate the signal outside the required perimeter.
- Take care with interferences between different networks in the same space. It

is possible to distribute the assignment of frequency bands between different infrastructures. The WLAN is also vulnerable to interference from other equipment (for example Bluetooth, microwave ovens, TV splitters, etc. or any transmission on the 2.4 GHz band).

Access points (AP terminals)

- Reduce the transmission power using a software command.
- Prefer to control parameter settings in local mode (for example through the serial port) and therefore avoid remote controls. This choice has to be made at the time of the purchase; the extra cost is about 5%. This administration mode introduces severe constraints if it is decided to use authentications through the MAC address or a RADIUS system, due to updates of lists (ACL). Interoperability problems may arise for equipment with different technologies.
- Activate the 104-bits, or even the 40-bits version of the WEP. The 40-bits version already includes some built-in hardening of security, although there is some software capable of crypto analysis of keys, even on WEP2.
- Choose a SSID: prevent public broadcasting that involves a longer distance broadcast. Choose a network name that is nothing like the company name or the activity name, to avoid arousing intrusion attempts. Do not leave the default SSID of the AP that will provide information about the make (and its vulnerabilities, if any). Also take care with the use of a DHCP server that invites any station belonging to the SSID group to make a connection.
- Filter by MAC address: this solution is only feasible for a small number of connected stations, otherwise it quickly becomes difficult to update the address tables.

Portable equipment

- Use a software command to activate BSS and ESS modes to prevent a connection on a fake AP terminal (man in the middle scenario).
- If portable equipment is not supposed to connect to a wireless network, it is preferable to deactivate the resource to prevent an accidental connection or a connection to a wrong AP terminal close to the company or in a public location. Depending on the equipment, move a jumper on the mother board, deactivate the resource in the BIOS or deactivate the peripheral driver within the operating system (for example, the default version of Windows XP includes management of wireless cards).

B) Reinforcement of security resources

The necessary actions are related to human, organizational and technical aspects.

Increased awareness by all users about the challenges

- The people concerned most closely are often computer scientists, salesmen, consultants, Management that may be attracted by a very easy-to-use technology. It is recommended that the deployment policy should be formally defined.
- Deployment of a domestic WLAN is another potential danger point for equipment that connects to it for business use. For example, if there is no security perimeter, directories in shared mode will be one means of accessing confidential information belonging to the company or the authority.

Dynamic change of WEP keys

The WEP key can be changed periodically to prevent or reduce interception possibilities. Although a portable station can often be used to make such a modification, other equipment such as tablets can cause problems. Interoperability of all equipment might be degraded.

Hardened authentication

- Set up a RADIUS system using a VPN, IPSEC architecture, etc.
- Use the 802.1x protocol (LEAP, PEAP) that requires more expertise.

RFC (Request for Comments) 2284 for EAP (Extensible Authentication Protocol) explains this standard for authentication, user control and online changes to encryption keys.

PEAP and TTLS are two concurrent standards proposed by different players to improve EAP.

Geopositioning of terminals

This mapping may be envisaged periodically. It requires the installation of GPS equipment to position the terminals.

Recording connection logs

Some terminals enable the transmission of logs for central processing. They will thus be saved for analyses of atypical situations.

Correction of software bugs

Software malfunctions, and even security weaknesses, may be corrected by updating AP terminal programs.

5. Regulatory framework

The ART (Autorité de Régulation des Télécoms) should be consulted periodically, since the legal framework changes.

Caution with audit actions: there is a risk of intrusion on another nearby WLAN. Therefore, it is essential to identify the network to be audited and to manipulate active scanners carefully, which by definition will insert themselves in all networks accessible within the surrounding space.

Also remember that a “bounce” attack is an opportunity; the WLAN will act as a first connection point for an attack on Internet. Therefore the Company or the authority itself is responsible for the dishonest act.

At the moment, there is no jurisprudence about application of deployment rules or dishonest actions done.

6. References

A) Regulations and security recommendations

http://www.etsi.org
http://www.art-telecom.fr/
http://standards.ieee.org/wireless
http://www.wi-fi.com/
http://www.hsc.fr/ressources/presentations/
http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/
http://www.weca.net

B) Attack software and procedures

http://www.netstumbler.com/
http://www.bretmounet.com/ApSniff/
http://wepcrack.sourceforge.net/
http://www.warchalking.org