

# FACTSHEET FS-2008-01

## Wireless networks

The introduction of wireless networks signified a breakthrough in the past in terms of connectivity and mobility of network users. Wireless networks can provide solutions for both home users and businesses, thanks to their great flexibility. There are of course risks involved, but a wireless connection can be made very secure by taking the right measures.

This fact sheet describes the main standards, technologies and safety aspects for Wi-Fi, the technology that is currently the most widely used for wireless networks.

Technologies such as Bluetooth, WiMAX and infrared fall outside the scope of this fact sheet and are not dealt with.

### Standards: 802.11x and Wi-Fi

Wi-Fi is a brand name that was created in 1999 by the Wi-Fi Alliance. It is intended to be a recognizable 'certificate' that can be displayed by products that comply with the IEEE series 802.11 standards<sup>1</sup> and which the alliance has tested for interoperability.

Digital signals are converted to make them suitable for sending using radio waves for the purposes of wireless network connections. Technologies based on 802.11 make use of the 2.4Ghz and 5Ghz wavelengths.

The most recent 802.11 standard is 802.11n. It offers the greatest speed with a guarantee of interoperability with other equipment.

The main feature of 802.11n as compared to older standards is the increase in the transfer speed to a theoretical maximum of approximately 300Mbps.

### An overview of the facts:

- > Wi-Fi: based on IEEE standard 802.11.
- > 802.11g currently dominates the market.
- > 802.11g has a theoretical transfer speed of 54Mbps. In practice only half this speed is possible.
- > 802.11n is the most recent standard. It offers a theoretical transfer speed of 300Mbps.
- > One cannot guarantee the availability of wireless connections.
- > For confidentiality and integrity: use WPA2 or another encryption standard.

### The main 802.11 standards are:

	Year	Wavelength	Speed	Comment
802.11a	1999	5Ghz	54Mbps	obsolete
802.11b	1999	2.4Ghz	11Mbps	obsolete
802.11g	2003	2.4Ghz	54Mbps	
802.11i	2004	n.a.	n.a.	security
802.11n	2009	2.4 and 5Ghz	300Mbps	

<sup>1</sup> This fact sheet does not deal with all the standards from the 802.11 series. The standards that are not mentioned describe aspects of wireless networks that are not considered here, such as bridge operations, quality of service and roaming. One can find a list of freely available standards at <http://standards.ieee.org/getieee802/802.11.html>. Other standards are only available for payment.

## Speed and coverage

The speed and coverage of a wireless network depend on a large number of factors, which makes it difficult to make generalizations.

It is generally true that the transfer speed of a wireless network decreases the greater the distance from the connection point (an access point, router or other computer). Therefore the greater the distance, the slower the speed.

A network based on 802.11g for example offers a theoretical transfer speed of 54Mbps. In practice only half this speed is possible for actual network traffic. Under normal circumstances it should be possible to make a connection over a distance of approximately 100 metres<sup>2</sup>, but at this distance the speed may be reduced to 1Mbps. A maximum distance of 25 metres is recommended for optimum speed<sup>3</sup>.

### Influences on wireless networks:

- > Objects such as trees and walls that are in the way.
- > Atmospheric conditions such as fog, rain and snow.
- > Interference from other devices such as microwave ovens, baby intercoms and household telephones.
- > The quality of aerials used by access points (network components) and clients (users).

Other figures apply to eavesdropping on wireless networks. Merely capturing wireless traffic, which does not require a connection to an access point, is possible up to far greater distances.

## Threats and solutions

The convenience of wireless computer networks must be viewed against certain risks that are inherent to the medium being used, namely radio signals.

### Availability

An important safety aspect of wireless networks is that their availability cannot be guaranteed. Their weakness is that the data is sent through the ether, which enables third parties to interfere with the signal<sup>4</sup>. In certain cases this does not even require any special equipment, thus making a deliberate attack quite easy<sup>5</sup>. There can also be unintentional interference or influences on the connection quality.

Do not solely rely on a wireless network in an environment where a high degree of reliability is required.

### Confidentiality and integrity

Standard wireless networks do not guarantee the integrity and reliability of data. Anyone can in any case capture and listen in to an unencrypted radio signal, and also manipulate it.

Encryption in combination with an authentication server can ensure that only authorized clients are able to connect to a wireless network and at the same time encrypt the traffic between the client and the access point. This latter point is significant. Wi-Fi encryption only has an effect on the radio signal. As soon as traffic enters the wired network it is unencrypted.

**Be careful:** To guarantee improved integrity and confidentiality of traffic, for example for teleworking, it will therefore be necessary to make use of additional measures, such as encryption in the form of VPNs, HTTPS or IP-SEC.

<sup>2</sup>Very powerful equipment can bridge much larger distances - up to several kilometres. This of course has implications as regards being able to eavesdrop on the signal.

<sup>3</sup>An informative overview of the range and strength of the 802.11a/b/g standards can be found on [www.cisco.com/en/US/products/hw/wireless/ps4570/products\\_white\\_paper09186a00801d61a3.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml)

<sup>4</sup>'SANDIA REPORT SAND2006-3517 EM Threat Analysis for Wireless Systems', June 2006, §2.2 and §2.3 <http://www.osti.gov/bridge/servlets/purl/889002-nS2W22/>

<sup>5</sup>See security advice in GOVCERT.NL-2004-131.

## Wireless security: WEP, WPA, WPA2, WPA-PSK, WPA-Enterprise, TKIP and AES

Various technologies are available for the encryption of wireless signals, as part of the wireless specifications, and various terms are used. The main ones are explained below:

- **WEP** (*Wired Equivalent Privacy*) was designed as part of the original 802.11 specification from 1999. WEP has been completely superseded as a security method. There are various tools available which make hacking WEP child's play.
- **WPA** (*Wi-Fi Protected Access*) is based on parts of 802.11i from 2004. WPA was introduced at the time as a temporary solution, because WEP turned out to be very weak. It was a precondition that WPA would work on the same hardware as WEP. Use was made for this purpose of TKIP (*Temporal Key Integrity Protocol*), an algorithm that used RC4, just as did WEP, but which solved certain weaknesses. In the meanwhile it has become clear that TKIP also has some minor vulnerabilities.
- **WPA2** is based on 802.11i from 2004 and is now the definitive standard, after WPA. WPA2 is compatible with WPA, but compared to TKIP includes a newer and more robust encryption method known as AES (*Advanced Encryption Standard*). WPA2 therefore in fact consists of WPA/TKIP and WPA/AES. Often the terms WPA and WPA2 are used indiscriminately, when only WPA2 is meant.
- **WPA-PSK** (or *WPA-Personal*) stands for *WPA-Pre-Shared Key* and is the term for the home version of both WPA and WPA2. In the case of WPA-PSK the wireless network makes use of a shared key. This key has to be entered on all devices: the access point and all devices that wish to connect to it. In the case of WPA-PSK it is possible to choose for both TKIP and AES. WPA-PSK is suitable for home use situations, but has certain disadvantages that make it less suitable for small or large organizations:
  - Traffic is encrypted, but only inasmuch as outsiders cannot listen in to it. Any devices that are connected to the wireless network can - by the use of a shared key - read each other's traffic!
  - WPA-PSK does not have any tools for key management, which can as a result become very complex and time-consuming where there are several devices and a lot of staff turnover.
- **WPA-Enterprise** is the business version of WPA. WPA-Enterprise does not make use of a shared key for encryption and access to the wireless network. Instead of this, use is made of an authentication server that ensures that a unique key is used for every device that is connected to the wireless network. In the case of WPA-Enterprise it is possible to opt for TKIP or AES.
- **TKIP** (*Temporal Key Integrity Protocol*) is the encryption algorithm found in both WPA and in WPA2. It was designed as a rapid replacement for WEP. The first feasible attack on TKIP was announced at the end of 2008<sup>6</sup>. This attack means that in most cases there is fortunately no great risk to a wireless network protected with TKIP, but it does mean that it would be advisable to transfer to AES.
- **AES** (*Advanced Encryption Standard*) is a robust encryption mechanism from 2001. It forms part of WPA2 (along with TKIP), but unlike TKIP requires somewhat faster hardware. AES is ideal for use with any hardware that is no more than about five years old.



Small or large organizations should use WPA2/AES in combination with an authentication server<sup>7</sup>. Only authorized clients can make a connection and system users cannot listen in on each other's traffic. Consider as well additional measures such as VPNs or HTTPS to encrypt traffic from end point to end point. At home select WPA2/AES with a strong (difficult) password with a minimum 14 characters. Avoid using WPA/TKIP.

<sup>6</sup>On 8 November 2008 two security researchers announced that they had succeeded in carrying out a feasible attack on TKIP. The details can be read in: <http://dl.aircrack-ng.org/breakingwepandwpa.pdf>

<sup>7</sup>When making use of an authentication server be careful about your choice of an authentication protocol.

### Additional measures

Setting up encryption for a wireless connection is an important measure, but not the only one you can take. We will list some further measures that are of importance in the context of wireless networks.

- Modify standard passwords on access points.
- Set up access points in such a way that the management interface is only accessible from the wired network.
- Switch uPnP off at access points. uPnP can be used to make unauthorized changes to the configuration of an access point.
- Include the firmware and drivers for your access points and wireless network cards in your patch management cycle.
- Make the settings on your access points part of your configuration management.
- Separate your wireless network from your wired network. The access point (and therefore the wireless network) must as a minimum be separated from your wired network by means of a firewall.
- Harden clients which make use of wireless networks.

### Disputed measures

Other measures are also regularly mentioned that are supposed to limit the risks of wireless networks. There are doubts about the effectiveness of these measures, certainly in relation to those already mentioned in this fact sheet.

- Switching off SSID broadcasting (the SSID is the name by which a wireless network can be recognized). This measure only suppresses two out of the five types of frames that a SSID may include and is not a security measure. We would counsel against this.
- It is not sensible to state the brand and version of the access point in a SSID. A descriptive SSID (for example the name of the organization) may have a lot of benefits from the viewpoint of user-friendliness compared to the marginal security value of a non-descriptive SSID. We advise making a well-considered decision in this regard.
- Spoofing of MAC addresses is a trivial matter. Filtering for MAC addresses therefore contributes little as a security measure and may entail high administrative burdens. It is best to think carefully before coming to a decision in this respect.
- Restricting the radio signal makes it easier to render a network less accessible. It is however difficult to determine the range of the signal in advance; this not only depends on the sender but also on the recipient. An attacker with very powerful equipment can capture a signal that would not be measurable with normal equipment. Think carefully before making a decision.

### Additional information

NIST SP 800-48: Guide to Securing Legacy IEEE 802.11 Wireless Networks  
<http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>

NIST SP-800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i  
<http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf>

Wi-Fi alliance Knowledge Centre, Security  
<http://www.wi-fi.org/searchresults.php?c=11&sp=Security>

Securing WLANs using 802.11i (draft)  
<http://csrc.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf>