



Security in wireless local area networks

Advice to users for improved security

Foreword

The National Post and Telecom Agency (PTS) has observed an increase in wireless local area networks. Not only is it possible to use wireless connections to the Internet at home and at work, they can also be used in public locations. Because of the increase in the number of wireless local area networks, PTS wishes to provide information about the vulnerabilities that exist as well as advice about the security measures that should be taken.

The Swedish Government has decided on a national strategy to improve Internet security. Part of the action plan is for PTS to provide information about vulnerabilities as well as coordinate and increase the number of information initiatives for users. This report is part of the national strategy to improve Internet security.

It was produced by Thorbjörn Blomdahl (project manager), Peder Cristvall, Erika Hersaeus, Björn Scharin and Roland Svahn (quality assurance).

Stockholm, June 2007

Marianne Treschow

Director-General

Contents

Summary (in Swedish)	9
Summary (in English)	11
1 This report describes how users of wireless local area networks can protect themselves against vulnerabilities	13
1.1 The mission of PTS is to inform users about vulnerabilities in wireless local area networks and to provide advice in order to minimise the impact of these vulnerabilities.....	13
1.2 The aim of this report is to describe how users can protect themselves when using wireless local area networks.....	14
1.3 This report focuses on WLAN technology.....	14
1.4 Users of wireless local area networks are the target group of this report.....	14
1.5 The report is based on a preliminary study, interviews, a field study and a literature study.....	15
1.6 Definitions of concepts used in the report.....	15
1.7 The structure of the report and reading instructions.....	16
2 Introduction to wireless local area networks from a technical, market and legal perspective	18
2.1 WLAN is the most common form of wireless technology for computers.....	18
2.2 Wireless local area networks transmit data using radio waves.....	19
2.3 Wireless local area networks consist of devices that have a network card for wireless transmission, an access point and a modem.....	19
2.4 IP addresses are needed so that data can arrive at the correct computer on the Internet.....	20
2.5 Solutions to improve security in wireless local area networks include authentication and encryption.....	20
2.5.1 Authentication means verifying identity and authorisation.....	21
2.5.2 Encryption is used to protect data being transmitted.....	21
2.6 The use of private wireless networks is becoming increasingly common.....	22
2.7 The market for public wireless networks is under development.....	22
2.8 Providers of wireless networks that constitute public communications services have a notification obligation vis-à-vis PTS.....	23
3 Vulnerabilities in wireless local area networks	25
3.1 Interception is the main risk when using wireless local area networks.....	25
3.2 Unauthorised parties can utilise the wireless local area network for their own purposes.....	26
3.3 Wireless products can cause interference.....	27
3.4 General risks when using the Internet include malicious codes, etc.....	27
4 Experiences gathered related to security in wireless local area networks	29
4.1 A slight improvement in security awareness among users of private wireless networks.....	29
4.2 Low security awareness among users of public wireless networks.....	30
4.3 There is a lack of information about the security level of public wireless networks.....	30
4.4 Few reported offences that are related to wireless local area networks.....	31
4.5 Up until now, security has had little impact on market developments.....	31
4.6 Public authorities and organisations in other countries provide advice related to the use of wireless local area networks.....	32

5	Trend toward more wireless local area networks and more products supporting this technology	35
5.1	The market for wireless technology will grow and expand in a society that is increasingly wireless and mobile.....	35
5.2	Security in public wireless networks will remain at a low level and it will take some time before service providers introduce standardised encryption solutions	37
5.3	Technology and terminal convergence means that the vulnerabilities of traditional computers are also present in mobile telephones and handheld computers	38
6	Security advice for users of wireless local area networks	39
6.1	Security advice when using private wireless networks.....	39
6.1.1	Disconnect the wireless local area network when it is not in use	40
6.1.2	Change the user name and password in new equipment for the wireless local area network	40
6.1.3	Change the name of the wireless local area network and disable automatic broadcasting of the name	40
6.1.4	Activate the most secure level of encryption permitted by the equipment.....	41
6.1.5	Decide which computers should have access to the wireless local area network	41
6.1.6	Use manually allocated IP addresses so that adjacent computers cannot connect to your network	42
6.1.7	Reduce the coverage of the wireless local area network.....	42
6.1.8	Change channels from the basic configuration on new equipment.....	43
6.2	Security advice for users of public wireless networks	43
6.2.1	Assume that all communication is unprotected and use a secure connection when dealing with sensitive information	44
6.2.2	Ensure that you do not unwittingly communicate with the outside world	45
6.2.3	Be aware of false access points.....	45
6.2.4	Be aware of social factors	45
6.3	General security advice when using the Internet.....	46
6.3.1	Ensure that you have an up-to-date firewall, antivirus program and operating system.....	46
6.3.2	Choose and use strong passwords	46
7	Positions adopted focussing on continued work	48
7.1	Service providers shall inform users about the level of security of the network and provide users with recommendations	48
7.2	Suppliers of equipment for wireless local area networks should facilitate security measures through improved factory settings and better user interfaces	48
7.3	Rules and information concerning the notification obligation under the Electronic Communications Act may be clarified in the light of new business models.....	49
7.4	Users of public wireless networks should request improved security	49
7.5	PTS will continue to provide information about security in wireless local area networks	49

Bibliography	51
1 Definitions of concepts	55
2 Explanations of abbreviations	60
1 Reading instructions	66
2 Description of the framework behind WLAN technology	66
2.1 Mesh networks comprise individual nodes which collectively establish wireless coverage over entire cities and support mobility.....	66
2.2 Summary of several standards within WLAN technology	67
3 Security solutions for wireless local area networks	67
3.1 Authentication verifies a given identity against a network.....	68
3.1.1 Authentication in large networks is performed by a central authentication server.....	68
3.1.2 Local authentication takes place using keys based on the router's password	68
3.1.3 Authentication using a shared key is common in simpler equipment.....	69
3.1.4 WEP: the first generation of encryption standard for wireless local area networks is easy to decrypt.....	69
3.1.5 802.11i: a standard produced to improve the security of wireless local area networks	70
3.1.6 WPA: the second generation of encryption standard is more secure than WEP, but insufficiently secure for today's market	70
3.1.7 WPA2: the third and latest generation's encryption standard is currently viewed as secure.....	71
1 Introduction	74
2 Notification obligation under EkomL	74
3 Important obligations ensuing from notification	74
4 The Personal Data Act regulates the processing of personal data where processing is not specifically regulated by EkomL	76
5 Different types of market stakeholder	77
5.1 Private users sharing access.....	77
5.2 Private users as part of a larger network with one key stakeholder.....	78
5.3 Traditional service providers: hotspots.....	79

1	This appendix describes the initiatives taken by some other countries and provides examples of practical advice provided to improve security in wireless local area networks	82
2	The information and advice provided in Norway is similar to that of PTS's materials.....	82
3	Denmark provides advice on wireless local area networks and Danish authorities will be placing greater demands on service providers.....	83
4	In Finland, the Ministry of Transport and Communications promotes improved data security within wireless networks	84
5	The United Kingdom has a government policy for public administrative use of wireless local area networks and a campaign about data security	85
6	Federal authorities in the United States provide advice to users of wireless local area networks with additional advice being offered by Internet service providers	87
7	Australian public authorities provide advice to government and the general public	89
8	A public authority in Canada provides advice to SMEs.....	90

Appendices

Appendix 1 – Definitions of concepts and abbreviations used.....	55
Appendix 2 – A technical description of wireless local area networks	65
Appendix 3 – Legal implications of the regulatory framework pertaining to wireless local area networks.....	73
Appendix 4 – An international perspective of initiatives and practical advice for improving the security in wireless local area networks	80

Summary (in Swedish)

Sårbarheterna i lokala trådlösa nät är främst avlyssning, obehörig åtkomst till nätet och störningseffekter. Dessa sårbarheter finns eftersom information i lokala trådlösa nät överförs med hjälp av radiovågor vilka går att fånga upp och informationen skickas ofta i klartext dvs. utan kryptering. I publika lokala trådlösa nät krypteras i regel inte information och i privata lokala trådlösa nät sker det vanligtvis först när användaren aktiverar kryptering.

Säkerhetsmedvetandet hos användare är lågt men har ökat något för privata lokala trådlösa nät. Information om säkerhetsnivån i publika lokala trådlösa nät är bristfällig. Säkerhet har haft liten påverkan på marknadsutvecklingen för publika lokala trådlösa nät. Utvecklingen går mot fler trådlösa nät och produkter som stödjer tekniken.

PTS har tagit fram råd för ökad säkerhet till användare av lokala trådlösa nät.

Råd vid användning av privata lokala trådlösa nät är

- att stänga av nätet när du inte använder det
- att ändra det förinställda användarnamnet och lösenordet för administration av nätet som finns vid leverans av utrustningen
- att ändra namnet på nätet och att stänga av den automatiska utsändningen av namnet
- att slå på den säkraste krypteringen som utrustningen tillåter
- att bestämma vilka datorer som ska ha tillgång till nätet
- att använda manuellt (statiskt) tilldelade IP-adresser så att inte närliggande datorer kan ansluta sig till ditt nät
- att minska täckningen på nätet
- att byta kanaler från grundinställningen som finns vid leverans av utrustningen.

Råd vid användning av publika lokala trådlösa nät är

- att utgå från att all kommunikation sker oskyddat och använd en säker förbindelse när du hanterar känslig information
- att säkerställa att du inte omedvetet kommunicerar med omvärlden
- att vara uppmärksam på falska accesspunkter och på sociala faktorer.

Generella råd vid användning av Internet är att ha uppdaterad brandvägg, antivirusprogram och operativsystem samt att använda starka lösenord.

PTS anser att tillhandahållare av publika lokala trådlösa nät ska upplysa om vilken säkerhet som finns i nätet och ge rekommendationer till användare. Användare bör i större utsträckning efterfråga säkerhet. Leverantörer av utrustning till trådlösa nät bör underlätta säkerhetsåtgärder genom bättre inställningar vid leverans. PTS kommer att fortsätta informera om säkerhet i lokala trådlösa nät..

Summary (in English)

Vulnerabilities in wireless local area networks mainly include eavesdropping, unauthorised access to the network and interference. These vulnerabilities arise since data in wireless local area networks is transmitted by means of radio waves, which can be intercepted, and the information is often sent as cleartext, that is, without encryption. In public wireless networks, data is usually not encrypted, and in private wireless networks, this usually takes place when users activate encryption.

Users have a low level of security awareness, but this has increased somewhat for private wireless networks. There is a lack of information as regards the security level of public wireless networks. Security issues have had little impact on market developments pertaining to public wireless networks. There is a trend toward more wireless local area networks and products that support this technology.

The National Post and Telecom Agency (PTS) has drawn up advice to increase the level of security for users of wireless local area networks.

Advice when using private wireless networks includes:

- disconnecting the network when it is not in use
- changing the preset user name and password in new equipment for administration of the network
- changing the name of the network and disconnecting automatic broadcasting of the name
- activating the most secure level of encryption permitted by the equipment
- deciding which computers should have access to the network
- using manual (statically) allocated IP addresses so that adjacent computers cannot connect to your network
- reducing coverage of the network
- changing channels from the basic configuration of new equipment

Advice when using public wireless networks includes:

- assuming that all communication is unprotected and using a secure connection when dealing with sensitive information
- ensuring that you are not unwittingly communicating with the outside world
- being aware of any false access points and social factors

It is generally recommended when using the Internet to have an up-to-date firewall, antivirus program and operating system as well as strong passwords. PTS considers that providers of public wireless networks must provide information about the level of security of the network and give recommendations to users. Users should demand security to a greater extent. Suppliers of equipment for wireless networks should facilitate security measures through better configurations in new equipment. PTS will continue to provide information about security in local wireless networks.

1 This report describes how users of wireless local area networks can protect themselves against vulnerabilities

Summary of Chapter 1

The aim of this report is to describe the risks present when using private and public wireless networks and to provide advice about how users can protect themselves against different vulnerabilities.

The report focuses on the wireless technology known as WLAN (Wireless Local Area Network). The reason for this is the increase in the number of products (laptop computers, handheld computers and mobile and IP telephones) that use this technology and the increase in the number of public and private wireless networks using WLAN technology.

The report describes the prerequisites for security in wireless local area networks from a technical, market and legal perspective, illustrates the vulnerabilities and experiences related to security in wireless local area networks, provides users with advice and indicates the potential for future work.

This chapter describes PTS's assignment (Section 1.1), the aim of the report (Section 1.2), the delimitations of the report (Section 1.3), the target group of the report (Section 1.4), the methods and sources on which the report is based (Section 1.5), definitions of concepts (Section 1.6) and lastly the structure of the report is described and reading instructions are provided (Section 1.7).

1.1 The mission of PTS is to inform users about vulnerabilities in wireless local area networks and to provide advice in order to minimise the impact of these vulnerabilities

PTS is the sector authority for electronic communications; one of its objectives is to work towards "sound security for and a high level of confidence in electronic data management as well as a robust Internet infrastructure".

In December 2006, the Swedish Government decided on a national strategy to increase the security of the Internet's infrastructure. This strategy is based on PTS's proposal entitled 'Strategy to improve Internet security in Sweden' (PTS-ER-2006:12). The measures contained in the strategy include PTS providing information about vulnerabilities as well as coordinating and increasing the number of information initiatives on the behalf of users. This is part of the public authority's work to promote sound security in accordance with the Government strategy to improve Internet security. PTS has produced this report on its own initiative for this very reason.

1.2 The aim of this report is to describe how users can protect themselves when using wireless local area networks

The aim of this report is to describe the risks that are present when using private and public wireless networks and to provide advice on how users can protect themselves against different vulnerabilities. This means that there is a need to describe wireless local area networks from a technical perspective, a market perspective and a legal perspective.

We have also observed a need to survey the different forms of wireless local area networks that are currently present on the market and the experiences gathered to date. We have drawn up our advice and arrived at the positions adopted by PTS on the basis of this.

1.3 This report focuses on WLAN technology

This report focuses on WLAN (Wireless Local Area Network) technology. The reason behind this is the increasing number of products (laptop computers, handheld computers and mobile and IP telephones) using this technology and the increasing number of public and private wireless networks using WLAN technology. The report focuses on the vulnerabilities that are currently present in these networks and those that will be found within the next few years.

This report does not encompass the security aspects of mobile networks. For information in this area, we recommend the report entitled 'Security threats to mobile telephony. An assessment of the current situation – winter 2005/2006' (PTS-ER-2006:18). The security aspects of wireless networks, such as RFID or Bluetooth, are not covered either. Vulnerabilities arising in connection with terminal and technological convergence are only discussed briefly, as are issues relating to suppliers of equipment for wireless local area networks.

The international perspective of public authority security work focuses on Nordic countries and English-speaking countries.

1.4 Users of wireless local area networks are the target group of this report

This report is intended for users of private and public wireless networks based on WLAN technology.

The main body of the text is intended for users of wireless local area networks who do not have specific advance knowledge of the field. The appendices are intended for those who wish to obtain more information about technology, law and international comparisons. Users include persons at home, at work, in public places or other locations who all utilise wireless local area networks.

1.5 The report is based on a preliminary study, interviews, a field study and a literature study

This report is based on various sources and methods. A preliminary study, entitled 'Security in wireless networks', was conducted by Netlight Consulting AB prior to this report, which was concluded in December 2006. This preliminary study serves as the basis of this report.

A number of public wireless network providers were interviewed in order to find out what they had experienced as regards security work and vulnerabilities in public wireless networks. These were TeliaSonera Sverige AB, The Cloud Networks Nordic AB, Sting Networks AB (in charge of operating Skype's public wireless network, Skype Zones), B2 Bredband AB, FON and Ericsson Sverige AB.

A small field study was conducted in central Stockholm to see how public wireless networks function from a user perspective. The study investigated the information that users are provided with pertaining to the fact that the networks are unencrypted and what this may mean to users.

A literature study has been conducted. Among other things, information was compiled from external reports and open sources.

An international overview was carried out regarding the initiatives taken and advice provided for increasing the security of wireless local area networks. This focussed on the Nordic countries and some English-speaking countries (Australia, Canada, the United Kingdom and the United States).

This report is a follow-up of PTS's previous information materials concerning security in wireless local area networks which have now been expanded by including public wireless networks. The previous materials are:

- a brochure entitled 'About wireless local area networks', which is directed at private users in home environments
- a report entitled 'Wireless networks, WLAN – a technical market report' from 2004 (PTS-ER-2004:12)
- PTS's website about Internet security, <http://www.pts.se/internetsakerhet/Sidor/startside.asp>, where information is provided for both home and work environments.

1.6 Definitions of concepts used in the report

The area discussed in the report is technical and encompasses many concepts and terms. Some of the concepts in the report have been replaced by simpler wording to make reading easier. For example:

- In this report, 'wireless local area networks' refer to local networks that use the wireless technology based on a standard called IEEE 802.11 and which is often known as WLAN (Wireless Local Area Network).
- In this report, 'private wireless networks' refer to wireless local area networks set up for private use in a home environment or at the workplace; for example, in business.
- In this report, 'public wireless networks' refer to wireless local area networks set up for public use.
- In this report, 'service providers' refer to market stakeholders offering public wireless networks on a commercial or non-commercial basis.
- In this report, 'security' refers to how users of a wireless Internet connection are to protect data on their computers, their private wireless networks as well as the data sent or received by users via wireless local area networks.
- In this report, 'vulnerability' refers to how Internet users may be subject to a number of threats specifically related to wireless communications and to Internet use in general.
- In this report, a 'network device' refers to, for example, a computer, a printer, a handheld computer or other device that has a network card that supports wireless communications in accordance with the WLAN standard.
- In this report, an 'access point' refers to a central node which directs the traffic in a wireless network and which grants or denies access to a wireless network.

Appendix 1 provides a more detailed account of the concepts and abbreviations used, including explanations.

1.7 The structure of the report and reading instructions

Each chapter begins with a box summarising the most important content so that the reader is given a quick overview. A description of the chapter's structure is provided under each box.

Chapter 1 initially describes PTS's assignment, followed by the aim, delimitations, methods, sources and target group of the report. Concepts used in the report are also defined; lastly, reading instructions are provided and the structure of the report is described.

Chapter 2 provides an introduction to wireless local area networks from different perspectives. Here, an overall technical description of wireless local area networks is provided in addition to an illustration of the current market and a legal

introduction to the obligations applying to end users as well as to service providers.

Chapter 3 describes the vulnerabilities present when wireless local area networks are used, both for private wireless networks and public wireless networks. The impact that a low level of security in these networks has is also described, as well as a presentation of the developmental trends affecting security within, and the market for, public wireless networks.

Chapter 4 presents the problems and security solutions that different market stakeholders and users have come across. Here, experiences from use of public wireless networks are described through field studies carried out by PTS and experiences gathered from the police and prosecutors, service providers of public wireless networks and Sitic, Sweden's IT Incident Centre. Lastly, this is followed by an overall international description of the advice provided to users of wireless local area networks around the world.

Chapter 5 describes the future prospects of wireless local area networks pertaining to the market, security and the possible risks that may arise within the next few years.

Chapter 6 provides users with advice about how to protect their computers, their wireless local area networks and their data when using public and private wireless networks.

Chapter 7 describes the positions adopted by PTS and continued work within the area.

The report has several appendices that apply to different areas. Appendix 1 contains explanations of the concepts and abbreviations used. Appendices 2 to 4 contain a more detailed account of technical, legal and international aspects.

2 Introduction to wireless local area networks from a technical, market and legal perspective

Summary of Chapter 2

'Wireless networks', referred to as 'wireless local area networks' in this report, usually refer to WLAN technology. This is a standardised technology that is common for computers, handheld computers and new telephones intended for wireless Internet use.

Radio waves are used to transmit data in wireless local area networks. Wireless local area networks consist of devices, such as laptops and desktop computers, with a network card that supports wireless data transmission in addition to an access point that receives the radio waves and controls and manages wireless access to the network. An Internet connection is also required, which is usually in the form of a modem.

Following the increase in the number of private wireless networks over the past few years, access to public wireless networks is also growing. The market for public wireless networks is relatively new and is expanding.

Parties providing a public electronic communications service, for example, a public wireless network, are required to notify PTS of this.

This chapter first describes the basics of wireless local area networks (Section 2.1). This is followed by a description of the technology, which will help the reader to understand the advice provided in Chapter 6 (Sections 2.2 to 2.6). Section 2.6 provides a description of the current use of wireless local area networks in homes and Section 2.7 provides a market-related presentation of public wireless networks. Section 2.8 contains a legal description of the provisions of the Electronic Communications Act (2003:389) as regards service providers.

2.1 WLAN is the most common form of wireless technology for computers

Wireless local area networks usually refer to the wireless technology known as WLAN. WLAN is an abbreviation of 'Wireless Local Area Network'.

Wireless local area networks are becoming increasingly common in homes, on campuses and at the workplace. They are also becoming more common in public places, such as restaurant and café chains, train stations, on trains and in public squares.

Private and public wireless networks are, for example, used to connect a laptop computer, a handheld computer or to place a call using an IP telephone (a WLAN telephone). Some newer, more advanced mobile telephones are also able to connect to the Internet via wireless local area networks. A private wireless network can be used to connect computers, printers and other devices to both it and the Internet.

2.2 Wireless local area networks transmit data using radio waves

Wireless local area networks transmit data using radio waves instead of a cable. For standardised WLAN technology, this means that the data is transmitted on the unlicensed 2.4 and 5 GHz frequency bands. The fact that these frequencies are unlicensed means that devices can transmit on these frequencies without the owner having to apply for a licence.

Wireless transmission has different ranges and transmission rates depending on the wireless standard integrated in a network device; generally, the newer the standard, the higher the transmission rate and the broader the range. Today, the *de facto* transmission standard for wireless devices is IEEE 802.11g. The Institute of Electrical and Electronics Engineers (IEEE) is the organisation that develops standards for this technology, which explains the name of the standard. IEEE 802.11g offers a transmission rate of 54 Mbit per second. The previous standard, IEEE 802.11b, offers a transmission rate of 11 Mbit per second. It is still being used since old devices with that standard are still in use on the market.

It is expected that the standard for the next generation's transmission rate will be ready in 2008 – IEEE 802.11n. It will offer rates of up to 100 Mbit per second. This year (2007), a few products are already implementing an early version of this standard.

The transmission rate in wireless local area networks is affected by the distance to the access point; the greater the distance, the lower the transmission rate.

The range of the wireless local area network depends on a number of factors. These include frequency, transmitter output capacity and natural barriers. A lower frequency provides a broader range and vice versa. In Europe, transmitter power may not exceed 100 mW EIRP (Equivalent Isotropically Radiated Power) in the 2.4 GHz frequency band.

See Appendix 2 for more detailed information concerning technical descriptions of wireless local area networks and their security.

2.3 Wireless local area networks consist of devices that have a network card for wireless transmission, an access point and a modem

Wireless local area networks using WLAN technology may arise in two ways; either through what is known as an 'infrastructure network' or through what is known as an 'ad hoc network'.

An infrastructure network is characterised by having central flow control. Central flow control occurs via the access point. An infrastructure network, which is the most common type of wireless local area network, consists of devices, such as laptops or desktop computers that have a network card supporting wireless data transmission as well as an access point. The access point receives radio waves, and controls and manages wireless access to the network. All of the traffic in an

infrastructure network has to pass the central point (the access point), even such traffic intended for other computers in the same wireless local area network.

Ad hoc networks do not have central flow control; that is, an access point. The ad hoc network consists of a computer connected to the Internet and a number of adjacent computers that communicate directly with one another without passing the central flow control.

Access points for private use have begun to develop into an 'all-in-one product' with both a router function and a built-in modem. The modem means that the access point/router is able to connect the computer to the Internet. The primary function of the router is to convey traffic to the correct computer in a network and to join networks together. Today, the concepts of routers and access points are often used synonymously, but a router is equipped with greater intelligence and functionality than a pure access point.

2.4 IP addresses are needed so that data can arrive at the correct computer on the Internet

Each device in a computer network has what is known as an 'IP address' (Internet Protocol address) so that the data being sent will arrive at the intended destination. Some IP addresses are globally unique and can thus be used on the Internet and be called public IP addresses. IP addresses that are only unique within a private network are known as private IP addresses and cannot be used on the Internet.

IP addresses can be allocated dynamically, that is, automatically, to network devices (e.g. computers) that are connected to a network. Alternatively, this allocation can take place statically through a manual procedure. This means that the address is entered using the keyboard before the device can be connected. Equipment such as access points and routers, or equipment which combines these functions, often has a DHCP server (Dynamic Host Configuration Protocol server) built in. This server can allocate the computers 'behind' the router on the home or corporate network with private IP addresses (i.e. internal IP addresses for the local network) when they connect to the network. Equipment that is directly connected to the Internet is usually given a public address by the Internet service provider. In addition, each network device has a globally unique identity through its network card. This identity is known as a MAC address (Media Access Control address). The equipment that allocates private IP addresses contains a table that translates private IP addresses into corresponding MAC addresses so that traffic can find the correct computer in the local network.

2.5 Solutions to improve security in wireless local area networks include authentication and encryption

There are a number of possible solutions to improve security in wireless local area networks; for example, authentication and encryption. These types of solution are described in this section.

2.5.1 Authentication means verifying identity and authorisation

Authentication means verifying the identity provided. Authentication is a common way to verify access. This may be done, for example, on the part of a user or by an access point.

The authentication of a user takes place in order to verify whether the user is authorised to use the network, the length of time the user may use the network, which services may be used, etc. Authentication is a type of access verification which grants or denies a certain user access to a network. The user must know the network password in order to gain access to the network.

An access point can be authenticated so that the user can determine whether or not the access point is genuine. An access point for a private wireless network is authenticated when the user, in his or her role as network administrator, has configured the access point with a network name (also known as an SSID, Service Set Identifier) and a password. In public wireless networks, users are often subject to authentication, but the reverse does not take place; in other words, the user does not authenticate the access point.

In public wireless networks, the users only see the network name (SSID) that the public network broadcasts, which means that users should ensure that the network is what it claims to be; i.e., that it is a genuine network.

2.5.2 Encryption is used to protect data being transmitted

Encryption is a method used to distort data in order to make it difficult for unauthorised parties to gain access to information through wiretapping. Encryption can also be used to protect a network from being used by unauthorised parties. Encryption and decryption between senders and receivers are carried out using what are known as 'keys'. These keys encrypt (distort) and decrypt data. The key for locking access to its network is often based on the password created by the user.

There are currently three standardised encryption methods for users of private wireless networks. These are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2 (Wi-Fi Protected Access 2). Different network devices support different types of encryption depending upon the age of the device. The oldest encryption method, WEP, is now considered to be insufficiently secure and can be decrypted within a few minutes using software that is readily available. WPA2 is the encryption standard that is currently viewed as being sufficiently secure against wiretapping.

Http (Hypertext transfer protocol) is a protocol for transmitting web pages from a server to a client (a computer) and is the most common protocol for Internet use. Https (Hypertext transfer protocol secure) is a more secure version of this protocol which encrypts the connection between two communicating parties, but not the content. Https is used, for example, by Internet banking services in order to ensure secure logging in and secure transactions.

VPN (Virtual Private Network) is another security solution for the Internet. A VPN connection encrypts data end-to-end between senders and receivers so that unauthorised parties cannot gain access to what is transmitted. Employers often offer corporate users such solutions so that they can securely log onto the corporate network and thus have secure access to the company's internal computer network and from there be able to securely utilise the Internet.

See Appendix 2 for more information about security solutions in wireless local area networks.

2.6 The use of private wireless networks is becoming increasingly common

The number of private wireless networks has increased each year since the first wireless LAN standard was developed in 1999. In Sweden, more than eight out of ten households currently have home access to the Internet. Twenty-seven per cent of those with home access to the Internet through a subscription paid for by the household have installed a wireless network in their home. This was revealed in the PTS report entitled 'Our demand for electronic communications - a Survey of Individuals' from December 2006. The users encompassed by this survey were between the ages of 16 and 75.

One factor behind the increased use of wireless local area networks is the greater use of laptops instead of desktop computers. Laptop computers often have built-in support for WLAN-type networks. Another contributory factor is the increase in 'all-in-one products' for Internet connection, with both a modem and wireless router in one device, which users can obtain from their Internet service provider.

2.7 The market for public wireless networks is under development

While wireless Internet use in the home is starting to become increasingly common, the market for public wireless networks is new and under development. Following a number of years of strong growth in private wireless networks, access to public wireless networks is now also increasing.

The market has changed since 2004, when PTS last conducted a market survey of service providers. Today, only a few of the service providers that were present in 2004 are still around. However, several new stakeholders have emerged. Telia Homerun and The Cloud are basically the only companies that have offered public wireless Internet connection since 2004. Examples of new stakeholders that have emerged in the market include Rover Rabbit, Skype with Skype Zones and Glocalnet with Glocal Zones. Competition between service providers is now increasing as regards the provision of public places with public wireless networks.

Another change since 2004 is that the number of access points in public places, i.e. hotspots, has increased considerably and there are currently a greater number of agreements with entire café, restaurant and hotel chains. There are also a few small public wireless networks, which are usually present in a few individual cafés, restaurants, hotels, etc., which offer wireless connection to the Internet.

One new form of wireless local area network has appeared on the market. It has meant that fixed broadband customers are beginning to share their broadband connections by opening up access to their private wireless networks. In this way, these users contribute to a user-generated wireless infrastructure. One example is the FON company, where users who share their Internet connections can also share some of its revenues.

2.8 Providers of wireless networks that constitute public communications services have a notification obligation vis-à-vis PTS

A party that provides a public electronic communications service is obliged to notify PTS of this. The aim of the notification obligation is, for example, to inform PTS about the stakeholders present in the Swedish market and to provide an opportunity to exercise supervision to ensure that they comply with the obligations ensuing from the Electronic Communications Act (2003:389) (EkomL).

An electronic communications service is defined as a service that is usually provided for payment and which entirely or primarily consists of the transmission of signals in an electronic communications network. For a service to be viewed as constituting an electronic communications service under EkomL, the service provider must, as considered by PTS, control in some way, either physically or in a legal sense (through ownership or agreement), some part of such transmission. If the transmission of signals takes place via a communications network or communications service that is completely independent of the service provider, which is unable to affect the preconditions for transmission, such as transmission capacity and quality, this service is not considered to be encompassed by the definition of an electronic communications service under EkomL. Networks that are provided solely for non-commercial use are not subject to the notification obligation. Private users who share an Internet connection via a wireless access point cannot be deemed to be providing an electronic communications service. In many cases, such a procedure may nevertheless contravene the subscription agreement applying to the subscriber in question. When it comes to service providers, it should be observed that the provisions of the Personal Data Act (1988:204) apply in those cases where EkomL does not specifically regulate certain processing of information that may be deemed to be personal data.

Those subject to the notification obligation and which provide public communications networks or public electronic communications services are obliged to, among other things, comply with the regulations contained in EkomL concerning operational reliability and the protection of privacy. For example, this means that the organisation must comply with reasonable requirements for sound function and technical security and reliability, as well as durability and availability. Furthermore, the provider must take appropriate measures to ensure that the data processed in the communications network is protected appropriately. The protection referred to includes protection against wiretapping and similar actions violating privacy. It follows from Chapter 6, Section 4 of EkomL that the service provider must also inform users about the risks and also, when necessary, provide

information about how to remedy risks and the approximate cost of such rectification. If the service provider does not offer encryption, for example, users should be informed about this and what this means.

See Appendix 3, Section 3 for a more detailed description of the regulatory framework pertaining to security in wireless local area networks.

3 Vulnerabilities in wireless local area networks

Summary of Chapter 3

Data in wireless local area networks is transmitted by means of radio waves, which can be intercepted relatively easily since the information is often sent as cleartext; that is, without encryption. Data in public wireless networks is usually not encrypted and data in private wireless networks is usually encrypted only once users have activated encryption themselves.

The main vulnerabilities that are specific to wireless local area networks are of three overall types: interception, unauthorised access to and use of a network using the identity of the network and interference.

This chapter describes the risks that are specific to wireless local area networks. Section 3.1 starts with an explanation of the main risk associated with wireless transmission. This is followed in Sections 3.2 and 3.3 by an account of the two next most common risks in wireless local area networks.

There are three overall types of risk in wireless local area networks. These are:

- an unauthorised party intercepting data transmitted to the access point via radio waves
- an unauthorised party gaining access to the network and utilising it for their own inappropriate purposes
- one or more adjacent wireless local area networks or other types of equipment using the same frequency band interfering with each other

These risks have different characteristics depending on the prerequisites of the different networks and arise from inadequacies in the design of the underlying protocols that enable wireless transmission using WLAN technology.

3.1 Interception is the main risk when using wireless local area networks

Data in wireless local area networks is transmitted using radio waves and may be intercepted at a distance of up to 100 metres. This range partly depends on the wireless standard that the access point (in the router) supports and partly on any barriers such as rock, hills, mountains or concrete walls. Furthermore, data transmitted in wireless local area networks is usually not encrypted; all of the data transmitted is sent to the access point in cleartext and can be intercepted during transmission, assuming that the connection to a website does not utilise the https protocol. Sensitive information, such as e-mail, user names and passwords for logging onto various e-services, can thus be intercepted by unauthorised parties.

A user with basic technical skills, using an ordinary computer equipped with a network card for wireless local area networks and readily available software, can

attack and access a protected network, even if it is protected with WEP encryption, the weakest method of encryption. Different types of radio equipment can intercept data as well.

One possible type of interception attack is what is known as a 'Man-in-the-Middle attack', where a device positions itself between the sender and receiver and intercepts the data. In this way, sensitive data for important e-services can be captured easily by unauthorised parties. A Man-in-the-Middle attack can take place both in the home and at public locations.

Another type of interception attack is what is known as an 'Evil Twinning attack'. An Evil Twinning attack means that a false access point is set up at a public location using the same network name (SSID) as an already well-known public local wireless network (hence the name) so that the user believes that it is a genuine network. False access points often broadcast with stronger signal strength than genuine ones so that computers connect to these. In this way, a false access point can intercept the unencrypted data. Public places can become particularly attractive interception locations where many users, both private and corporate, can be found, including public squares, airports and central train stations. Sitic, the Swedish IT Incident Centre, has confirmed that an Evil Twinning attack has been discovered at an international airport.

Moreover, data sent in a private wireless network can be intercepted by an unauthorised party, as a new wireless router does not have encryption activated and because radio waves can penetrate walls and floors.

Another potential risk in a private wireless network is if the user utilises WEP, which is the weakest encryption standard. Data encrypted using WEP can be decrypted in a few minutes using readily available software.

When it comes to interception, there are two overall threats. These are threats to privacy and threats to data security. Since the difference between work and leisure time is becoming increasingly blurred, laptops from work will be used for private errands and private computers will be used for work-related tasks (e.g. reading webmail). This affects data security and will place greater demands on clear regulatory frameworks for what users can and cannot do with their work equipment. When using a laptop computer in a wireless network, either a private or public network, a user should exercise caution for data security reasons if the computer contains sensitive information in the form of files, e-mail messages, etc., or when transmitting these.

3.2 Unauthorised parties can utilise the wireless local area network for their own purposes

The more private wireless networks are set up, the greater the likelihood that the wireless local area networks will become subject to interception or attempts by an unauthorised party to use the Internet, which is known as 'piggybacking'. If a user has not created a password or if a user has a password to the wireless local area network that is 'too weak', this may lead to interception or unauthorised access to and use of a wireless local area network. There is consequently a considerable risk

of intruders attempting to gain access to the network and utilisation of the user's Internet subscription; i.e. piggybacking. As regards passwords to a network that are 'too weak', e.g. in the form of proper names, surnames and common words, there are types of attack that use names and/or glossaries in order to access networks. In a worst case scenario, the unauthorised party may use the network to carry out a criminal act, such as downloading material subject to copyright, or child pornography.

In a wireless local area network (private or public) with no login verification, i.e. without authentication, unauthorised parties can use the network for their own purposes and thus use its anonymity to carry out criminal acts.

As authentication of access points (verification of access points; see Section 2.5 for more information) in public wireless networks does not usually take place, this may lead to an Evil Twinning attack; see Section 3.1 for more information.

3.3 Wireless products can cause interference

The more wireless local area networks that are set up, the greater the likelihood of interference in wireless local area networks. Not only computers, handheld computers, etc., communicate wirelessly on the 2.4 GHz frequency band. Examples of other products using this band include microwave ovens, remote controls, radio-controlled toys, wireless keyboards, headphones and digital video transmission. Radio interference between private wireless networks or as a result of products using the 2.4 GHz frequency band may affect both the range of the network and its transmission capacity. Channels have been introduced so that all devices using this frequency band will not interfere with one another when they are within each other's range. There are 14 channels in the 2.4 and 5 GHz frequency bands in Sweden.

Correspondingly, service providers may cause interference when setting up access points at public places since they all use the 2.4 GHz band. According to information from service providers, one of the principal requirements for public places is for the first stakeholder to set the channels on which its public wireless network is to transmit. This means that it can become difficult for competitors to introduce additional access points.

3.4 General risks when using the Internet include malicious codes, etc.

General risks when using the Internet include the user being affected by malicious codes, such as Trojans and viruses. A malicious code may, for example, delete, modify, copy or steal data from your hard drive or use your computer to help carry out what is known as a 'botnet attack', a common form of attack today. A botnet attack uses your computer to send out large quantities of data to a specific target, a specific computer or a specific Internet service in order to disrupt its function. Users are often unaware that they are involved in a botnet attack.

See, for example, PTS's website regarding Internet security (<http://www.pts.se/internetsakerhet/Sidor/startside.asp>) for more information

about general risks and threats when using the Internet. PTS has published many different reports. Examples include 'Strategy to improve Internet security in Sweden' (PTS-ER-2006:12) and 'Spyware and closely related phenomena' (PTS-ER-2005:15).

4 Experiences gathered related to security in wireless local area networks

Summary of Chapter 4

Users have low security awareness, but this has improved somewhat in terms of private local area networks.

There is a lack of information about the level of security of public wireless networks.

Few offences have been reported that are related to wireless local area networks.

Service providers have stated that security has not been a problem to date.

Up until now, security has had little impact on market developments pertaining to public wireless networks.

Public authorities in other countries often provide advice related to the use of wireless local area networks.

This Chapter starts by describing the users' level of security awareness related to private wireless networks (Section 4.1). This is followed by a corresponding discussion about public wireless networks (Section 4.2), followed by a description of users' experiences from public wireless networks (Section 4.3). Section 4.4 describes the experiences relayed by a number of service providers related to security in public wireless networks and Section 4.5 describes the experiences of public authorities related to security in wireless local area networks. This is concluded by a presentation of the advice provided to users of wireless local area networks by public authorities and organisations around the world (Section 4.6).

4.1 A slight improvement in security awareness among users of private wireless networks

Almost nine out of ten users have taken some form of measure to protect the computer used by their household. The same survey shows that 70 per cent of those with an Internet subscription use an antivirus program, 55 per cent use a firewall and 27 per cent use a security package from the service provider of the fixed Internet connection. A security package usually includes an antivirus program and a firewall. Of those with an Internet subscription, 32 per cent ensure that they update the computer's operating system. Twelve per cent of those with an Internet subscription have a protected wireless network "that unauthorised parties cannot gain access to". These statistics are the result of PTS's survey conducted in December 2006 entitled 'Our demand for electronic information' (PTS-ER-2006:47).

A number of studies have been conducted about the security level of wireless local area networks, for example by universities and colleges. A thesis was presented at Växjö University in June 2006 entitled 'The wireless society: an

investigation of the legal situation, the security situation and security awareness when using wireless home networks'. This study included their own investigations in Växjö, and also referred to previous investigations carried out in Linköping in 2003, in Jönköping in 2005 as well as in Phoenix in the United States in 2004. All of these investigations suggest an improvement in security awareness as regards wireless local area networks in home environments. The conclusion from the Swedish investigations is that the proportion of users encrypting their wireless local area networks in home environments increased between 2003 and 2006.

Sitc, Sweden's IT Incident Centre, whose mission is to provide information about threats, attacks and vulnerabilities on the Internet, has confirmed the general picture of improved awareness of security issues related to wireless local area networks, particularly encryption use in wireless local area networks in the home.

4.2 Low security awareness among users of public wireless networks

The security awareness of users of public wireless networks is likely to be fairly low, as the phenomenon of public wireless networks is relatively new. The number of private customers in public wireless networks is currently on the increase. They are less capable of protecting themselves and often lack awareness of risks and protective measures when using public wireless networks. It is likely that users assume the level of security to be the same as on the ordinary wired Internet. On the contrary, wireless local area networks are actually more vulnerable than the wired Internet since the data transmitted is completely unprotected and is relatively easy to intercept (see Section 3.1).

Users of public wireless networks generally have a higher level of security awareness when gaining access to their employers' e-mail and internal data networks. This is shown, for example, by the use of secure connections in the form of VPN tunnels; see Section 4.5.

4.3 There is a lack of information about the security level of public wireless networks

The field study carried out by PTS shows that there is a lack of information or none provided whatsoever about the level of security when using the Internet in public wireless networks. The various service providers of public wireless networks offer different solutions for Internet access and provide a variety of information about the security situation.

Only a small number of service providers inform users about the security level of their networks, and if users wish to make use of this security information, they must know where to look and must search for the information on the service providers' websites themselves.

Service providers offer wireless Internet in different ways, free and without user login, or alternatively logging in that is limited in time from 30 minutes up to a month, for a charge and using login details. In some cases, users can purchase access rights in a shop for a limited period of time where the user receives login

details in the form of a 'scratch card'; here, there is no registration of the purchaser of this service. In certain cases, users can purchase wireless Internet access via an SMS service from the service provider's start page on the Internet. There is no rigorous authentication of users, particularly as regards 'scratch cards' and purchases via an SMS service, which means that there is a lower level of security in these cases. When using a credit card, there is usually only one verification as to whether or not the credit card has been blocked, which also does not mean a high level of user authentication.

4.4 Few reported offences that are related to wireless local area networks

According to information provided by the police and prosecution authorities, no penal decisions have yet had a bearing on wireless local area networks. However, in a small number of cases in Sweden, there are indications that unprotected access points may have been used in order to commit offences. So far, there are no known legal cases where, for example, the identity or credit card details of a user were stolen in connection with their use of wireless local area networks. Examples of possible reasons for the lack of legal cases may be due to:

- users/network owners not having discovered security problems in wireless local area networks
- users/network owners not having reported any security problems in connection with wireless local area networks to the police
- up until now, there have only been very few security problems in wireless local area networks
- users/network owners are not bothered about whether someone has, for example, used wireless local area networks for piggybacking as long as it does not disrupt their own activities.

4.5 Up until now, security has had little impact on market developments

Interviews with service providers have shown that security up until now has not been a problem in public wireless networks. The factors behind the market development of public wireless networks are, in descending order, from the most important factor:

1. coverage
2. price
3. simplicity of connection and management
4. services, both content and capacity (transmission rate and range)
5. security

Up until now, most of those using public wireless networks have been corporate customers, who are security conscious. To date, those who request greater security are usually corporate customers, who generally utilise the company's own security solutions, such as VPN. One large service provider states that around 80 per cent of its traffic consists of encrypted traffic via users' VPN solutions.

The service providers state that up until now they have not experienced any problems directly related to security in wireless local area networks. Some service providers state that they are presently conducting tests of WPA-encrypted connections. One problem is the development of such software (referred to as 'clients') for laptop computers supporting WPA and newer and more powerful authentication solutions. At the same time, however, other service providers emphasise that they do not currently use encryption and are not presently planning to offer it in the future either.

4.6 Public authorities and organisations in other countries provide advice related to the use of wireless local area networks

Public authorities or other organisations in a number of countries provide advice related to the use of wireless local area networks. It is most common for a review to be conducted to identify potential threats and risks when using wireless local area networks as well as to provide examples of how users can protect themselves and what users need to bear in mind. Several of these examples serve as advice on how users should set up a wireless local area network in their home in a secure way. However, a number of organisations provide advice about what users should bear in mind in connection with their use of public wireless networks. As regards such networks, it is pointed out that it is important to understand that the level of security is lower when using public wireless networks and that it is safest to assume that they are not secure, which means that users should be cautious. Also, some emphasise that users cannot directly influence security in public wireless networks. A summary of the most important pieces of advice given about both private and public wireless networks is provided below.

The following advice is provided as regards private wireless networks:

1. changing user names and passwords for administration of the wireless router. If possible, disable the possibility of administering the wireless router from a distance
2. using MAC filtering to control access to the network
3. activating encryption and using the strongest possible (password?? – word missing??)
4. disconnecting the wireless local area network when it is not in use. A function in the wireless router could be used which limits the periods of time when it is activated
5. changing the name of the network

6. disconnecting the broadcasting of the network name (this type of broadcasting is also known as a 'broadcast signal')
7. verifying that equipment has CE marking
8. keeping the program (firmware) for the wireless router up-to-date
9. disconnecting the access point function for responding to queries by sending a 'broadcast message' about the network (which, for example, contains the network name (SSID)).
10. changing the shared crypto key regularly
11. restricting the coverage of the wireless local area network; for example, by the positioning of the wireless router and by using directional antennae
12. only using access points for connection and not ad hoc networks
13. using a secure connection when sensitive data needs to be sent or received; for example, via https or VPN
14. ensuring that crypto keys are configured for dynamic replacement
15. implementing suitable mechanisms for authentication; for example, RADIUS authentication (see Appendix 2 for more information)
16. adjusting the signal strength of the transmitter
17. companies should also monitor their wireless local area networks and be aware of employees who connect private equipment in order to set up wireless local area networks

The following advice is provided as regards public wireless networks:

1. there is a greater risk of the data being potentially intercepted and interpreted in public networks, as encryption is uncommon
2. as for all Internet use, the computer that you use must have an up-to-date operating system, an up-to-date firewall and an up-to-date antivirus program
3. asking the provider about the security mechanisms offered in public wireless networks
4. only using wireless local area networks managed by trusted service providers
5. if sensitive data is to be exchanged with websites, verifying that the transmission is protected through encryption (https)

6. if your computer is to be connected to your workplace, protecting the connection to your employer's network through encryption, that is, VPN.

See Appendix 4 for more information about the initiatives and practical advice provided in a number of countries for improving the level of security in wireless local area networks.

5 Trend toward more wireless local area networks and more products supporting this technology

Summary of Chapter 5

The market for wireless technology will grow within the next few years and society will develop into a more wireless and mobile world.

Security in wireless local area networks will remain low over the next few years and it will take some time before service providers introduce standardised encryption solutions.

The technology and terminal convergence that is taking place means that the vulnerabilities usually affecting computers will also affect mobile telephones and handheld computers.

This chapter illustrates the potential market for wireless technology within the next few years (Section 5.1), as well as how security in WLANs will develop (Section 5.2). This is concluded with a description of the threats arising through the convergence of technology, access lines and terminals that is underway (Section 5.3).

5.1 The market for wireless technology will grow and expand in a society that is increasingly wireless and mobile

The wireless technologies that will be available on the market within the next few years will largely be those that are already there now; that is, GSM, 3G (mobile networks), WLAN (wireless local area networks) and WiMAX (wireless broadband).

A continued rollout of public wireless networks will take place within the next few years. Continued investment in these networks can be observed, as service providers are in the process of developing content services in these networks. Examples of content services include being able to make video telephone calls, play games and connect to the network without an authentication solution (logging in). The impetus behind the development of public wireless networks includes the increase in sales of laptop computers, our increased need for the Internet, the fact that we are becoming increasingly mobile in our work and during our leisure time and also easier access to the Internet through handheld computers and certain mobile telephones that currently have built-in support for WLAN technology.

There has been a vision of a wireless society for some time now. This wireless society will soon be here. Not only are public wireless networks being offered through single access points at certain cafés, restaurants and hotels, but service providers have now concluded agreements with entire hotel, restaurant, newsstand and café chains. Ports, railways, train stations and airports have also been equipped with public wireless networks. In the future, it is likely that more wireless local area networks will be set up in the form of what is known as 'mesh

networks'. There are already examples of wireless urban networks that have been set up using this technology both in Sweden and abroad; for example, in Karlskrona. The mesh network can provide wireless coverage over large areas and support the mobility of users. See Appendix 2 for more information about mesh networks.

It is likely that there will be an increase in Internet telephony use in wireless local area networks; this is known as IP-based telephony. It has already become a new trend. Many see IP-based telephony as something that may further fuel the development of public wireless networks. One clear example of this application is Skype, which has developed an IP telephone for use in its public wireless networks, Skype Zones. If an IP telephone user is to be able to move about without interruption during an Internet telephony call, some functionality must be improved in the wireless local area networks, which is already currently available in mobile networks. This mainly applies to handover and roaming functionality. These are intended to enable mobility within a stakeholder's own wireless local area network and between the wireless local area networks of different stakeholders without interruption.

It is possible that we will see the continued development of user-generated infrastructure, such as FON. It is also possible that this will be offered by other stakeholders, such as the broadband providers themselves.

The main competitors in terms of WLAN technology are mobile telephone networks using 3G technology. Instead of investing in public wireless networks, a number of stakeholders are currently offering Portable 3G and Turbo 3G USB modems so that they can offer mobile and wireless Internet connection via mobile networks. Data traffic in the 3G networks has taken off. The computers connected are contributing to the increase in traffic, not the mobile telephone services. These portable USB modems can offer transmission rates of 3.6 Mbit per second if Turbo 3G technology is used. In practice, they achieve between 2.5 to 3 Mbit per second. However, the coverage for Turbo 3G is still limited and users outside major Swedish cities will have to settle for connection via the ordinary 3G network at a maximum rate of 0.384 Mbit per second. However, in the near future, 3G technology will be able to offer transmission rates of 14.4 Mbit per second. WLAN technology manages transmission rates of between 11 and 100 Mbit per second.

Wireless broadband technology and the WiMAX standard have been around for a number of years now, but this year investment in this technology seems to have taken off. WiMAX is a technology that can offer wireless broadband at distances of several kilometres. The telecommunications companies Motorola and Samsung, and the processor manufacturer Intel have chosen to invest in WiMAX. Ericsson, however, has chosen to discontinue its WiMAX research. Intel is pursuing the development of WiMAX by planning to integrate a WiMAX chip into computers in the future. WiMAX has currently been rolled out as an access network in a few locations in Sweden; for example, in the Municipality of Värmdö including a large number of the surrounding archipelago islands. In order to receive wireless broadband via WiMAX, users must first apply for a licence since this technology utilises a licensed frequency band, and then install a WiMAX

receiver on their roof. A wired (LAN) or a wireless connection (WLAN) is then used to connect to the Internet from this access point. It remains to be seen how the use of WiMAX will develop.

5.2 Security in public wireless networks will remain at a low level and it will take some time before service providers introduce standardised encryption solutions

It is likely that most public wireless networks will remain unencrypted over the next few years. There are standardised security solutions that encrypt networks for public wireless networks, such as the WPA2 standard. However, user-friendly programs for key management and the latest authentication methods must be supported by the different operating systems.

Some service providers are likely both to test and offer different encryption solutions to users commercially, whereas others will continue to have unencrypted networks. This depends on a balance between the simplicity of using the service, the security solution and the cost. However, if users increasingly requested greater security, this could speed up security development in the public wireless networks.

The presence of a large number of public wireless networks is a new phenomenon and the influx of wireless Internet customers may increase considerably as more wireless networks are provided in many more places. This may also lead to an increasing number of criminals using this network to intercept information. On the one hand, it is conceivable that interception becomes of particular interest in public places where there are many business travellers. On the other hand, ordinary private users could be monitored because they are unaware of the vulnerabilities or do not have access to a secure connection in the form of a VPN. Furthermore, the number of offences may increase as users become increasingly anonymous in the networks of certain service providers since authentication (user login) is not always conducted, because when accessing a network, simplicity is attributed particular value.

In the future, public network service providers may not only compete on the basis of price and availability (good coverage), but also on the basis of security. As a trade organisation behind the development of WLAN, the Wi-Fi Alliance has developed 'Best Practices', corresponding to general advice, for service providers of public wireless networks regarding how security should be implemented in such networks. Only one established service provider of a public wireless network can currently offer an encrypted network.

Regardless of how public wireless networks develop, the impetus for development in the near future is also likely to prioritise the following in order of importance: coverage, price, simplicity, service content, service capacity and, last of all, security.

5.3 Technology and terminal convergence means that the vulnerabilities of traditional computers are also present in mobile telephones and handheld computers

Technological progress means that different technical solutions and forms of access are undergoing integration. A convergence of technology, terminals and access lines is now underway. This means that several different access technologies are being integrated in the same product, for example, GSM/3G/WLAN, and that the terminals are being provided with an increasing number of functions, such as mobile telephones with cameras, music players, GPS navigators, etc.

In the near future, there will be an increasing number of users with smartphones. Smartphones are advanced mobile telephones that are capable of connecting to the Internet using different forms of radio technology. Connection to the Internet will not only take place via the GSM and 3G mobile networks and using WLAN, but also via Bluetooth and possibly also via WiMAX. An important aspect for the data security of smartphones and handheld computers is that they have considerably weaker processors compared with laptop computers, which will mean that their capacity to manage encryption is limited.

6 Security advice for users of wireless local area networks

Summary of Chapter 6

Security advice for users of private wireless networks includes:

- disconnecting the network when it is not in use
- changing the preset user name and password in new equipment for administration of the wireless local area network
- changing the name of the network (SSID) and disconnecting automatic broadcasting of the name
- activating the most secure level of encryption permitted by the equipment
- deciding which computers should have access to the network
- using manually (statically) allocated IP addresses so that adjacent computers cannot connect to your network
- reducing coverage of the network
- changing channels from the basic configuration on new equipment.

Security advice for users of public wireless networks includes:

- assuming that all communication is unprotected and using a secure connection when dealing with sensitive information
- ensuring that you are not unwittingly communicating with the outside world
- being alert to any false access points and social factors

When using the Internet, an up-to-date firewall, antivirus program and operating system are generally recommended as well as using strong passwords.

This chapter offers advice to users of wireless local area networks in order to protect their computer, their network and their data. First we present advice for improved security when using private wireless networks (Section 6.1), then we offer advice that applies when using public wireless networks (Section 6.2) and lastly a number of general pieces of advice relating to all Internet use (Section 6.3).

6.1 Security advice when using private wireless networks

PTS offers advice to users of private wireless networks. Protection of their private wireless network and the access to this network is the main area of vulnerability that users want to protect themselves against. The general advice provided in Section 6.3 should also be taken into consideration for private wireless networks.

6.1.1 Disconnect the wireless local area network when it is not in use

One basic piece of advice is to always disconnect the wireless router when the network is not being used, otherwise the network will continue to broadcast and receive radio signals and communicate that it is available.

You disconnect the network by disconnecting the power supply to the wireless local area network. If your wireless router does not have an on/off switch, we recommend that you pull out the cord or use a multiple socket with an on/off switch. Alternatively, a timer can be used to control when the network should be activated.

Disconnecting your wireless local area network means that there is no opportunity for an unauthorised party to monitor the wireless local area network or to connect to the network. This also reduces the risk of your wireless local area network causing a neighbour radio interference. See Sections 3.1, 3.2 and 3.3 for more information about the risks of wireless local area networks.

6.1.2 Change the user name and password in new equipment for the wireless local area network

You should change the user name and password for the wireless local area network (the wireless router) that are preset by the supplier of new equipment. Choose and use a good password, as described in Section 6.3.2.

In order to manage (administer and configure) your wireless local area network at home, you will need a user name and password. The new equipment will include a basic configuration with a user name and password. As a rule, a supplier has the same user name and password for all of its wireless routers. Different manufacturers have different standard values and these are easily found on the Internet. A wireless network transmits data about the manufacturer of the equipment and this information makes it easy to guess the user name and password being used.

Changing the user name and password makes it more difficult for someone else to take over and control your wireless local area network. See Section 3.2 for more information about the risks related to access by intruders.

6.1.3 Change the name of the wireless local area network and disable automatic broadcasting of the name

Change the name of the wireless local area network (SSID) and disable automatic broadcasting of the name. As a basic configuration, all wireless local area networks transmit their name, which in connection with new equipment is usually the name of the manufacturer or service provider. This is like a calling signal, which transmits and indicates that there is an access point seeking a party who wishes to connect to it. In a home wireless network, this function is only useful when the network is set up for the first time and the different devices in the wireless local area network are introduced to each other. You must know the name of the network in advance in order to connect to the wireless local area network.

You should change the name into something unique in order to ensure that you are connecting to your access point, and in order to protect it from other users. Your wireless local area network does not need a network name in order to work. After the different devices have been introduced to each other, you can disconnect the automatic broadcasting of the name on your wireless local area network. When you change or remove the name of the network, you must also do so in the computer, otherwise the network will not function. These changes are made in the wireless router. In order to do this, you need to log onto it by indicating your user name and password.

Changing the name of your wireless local area network and disabling the automatic broadcasting its name makes it more difficult for unauthorised parties to gain access to your wireless local area network. It also makes it more difficult for unauthorised parties to monitor your wireless local area network. See risks in Sections 3.1 and 3.2.

6.1.4 Activate the most secure level of encryption permitted by the equipment

You should activate the router's built-in encryption function. There are currently three different types of encryption method – WEP, WPA and WPA2. The weakest form of encryption is WEP, which is relatively easy to crack, but it does protect against spontaneous monitoring and access by intruders. WPA is significantly more secure than WEP, but not as secure as WPA2.

Not all wireless routers support all encryption methods. Use the strongest form of encryption supported by your router and network devices. If you encrypt using WEP, you should use a 128-bit encryption key. Remember to upgrade your router software regularly for improved functionality and security; for example, support for improved encryption. The latest software is often available for downloading from the manufacturer's website.

Using encryption makes it more difficult for unauthorised parties to intercept data that has been transmitted wirelessly in the network. See Section 3.1 for more information about risks in wireless local area networks.

6.1.5 Decide which computers should have access to the wireless local area network

All network cards, which are, for example, used in computers, have a unique number. This number is known as the 'MAC address'. You can decide which network cards are to have access to your non-public network by using a function in the wireless router known as 'MAC address filtering'.

In order to decide which network cards, and consequently computers, should have access to your wireless local area network, log onto your wireless router using your user name and password. Then activate the MAC address filtering function and indicate which MAC addresses are to have access to your wireless local area network.

However, advanced intruders can intercept which MAC addresses are approved in a wireless network and then change their own connecting equipment to have an approved MAC address so that they can penetrate your wireless local area network. Carrying this out requires some equipment, skill and a directed attack from an intruder.

Using MAC address filtering to determine which network cards should have access to the wireless local area network reduces the risk of unauthorised parties gaining access to your wireless local area network. However, it should be borne in mind that MAC address filtering is an unreliable method to be used as the only authentication method for access to your network. See Section 3.2 for more information about risks.

6.1.6 Use manually allocated IP addresses so that adjacent computers cannot connect to your network

Use manually allocated, static IP addresses instead of dynamic ones. All devices belonging to a network have an IP address. The IP address is the device's unique address and is used when it receives or transmits data over the Internet.

An IP address can either be allocated statically before connection to the network is made or dynamically in conjunction with connection. Today, access points and routers often have a built-in DHCP server, which means that they can allocate IP addresses dynamically. It is relatively convenient to allow the router's DHCP server to dynamically allocate an IP address to all devices connected to the wireless network, but this also presents a security risk. If it is easy to obtain an IP address, it is also easier to connect to the network. If a router or firewall is used, filtering can allow only legitimate IP addresses to access the network. However, just as for MAC addresses, traffic in the wireless local area network can be intercepted and IP addresses stolen, known as 'spoofing', so that penetration is made possible. However, carrying this out successfully requires equipment, skills and a directed attack from an intruder.

In order to use static allocation of IP addresses, you need to log onto your wireless router using your user name and password. Then activate the static IP address function.

Using static IP addresses reduces the risk of an unauthorised party gaining access to your wireless local area network. See Section 3.2 for more information about risks related to intrusion.

6.1.7 Reduce the coverage of the wireless local area network

Reduce the coverage of the wireless local area network. As a user, you have the opportunity to influence the range of your wireless local area network; that is, the coverage of your network. However, bear in mind that a certain signal, regardless of how weak it is, can always be traced. Even at low signal levels, most wireless networks can be traced using a sufficiently sensitive receiver and a good antenna.

The output capacity of most access points can be reduced in order to reduce coverage. The access point's settings can be changed. In order to reduce the output capacity of your wireless router, start by logging onto your wireless router with your user name and password and then change the output capacity so that it is sufficient for your needs. Moving the wireless router to a more central location in your home to reduce needless transmission outside the walls of your home is an additional measure for reducing and adjusting the coverage to suit your needs.

Reducing the coverage reduces the exposure of your wireless local area network to the outside world and consequently reduces the risk of it being subject to vulnerabilities such as interception and unauthorised access. See Sections 3.1 and 3.2 for more information about risks.

6.1.8 Change channels from the basic configuration on new equipment

Change channels from the basic configuration on new equipment. Wireless local area network devices usually transmit on the 2.4 GHz frequency band. This frequency band can be separated into several channels so that several wireless local area networks can coexist in the same area without causing interference. Your wireless router comes with specific pre-configurations, among them a channel (specified frequencies) that it uses for its communication. You can change the channel that you use in your wireless local area network to reduce the risk of interference. Change to a randomly chosen channel and test this channel. However, this change will require a degree of caution and individual testing in order to achieve a good solution as adjacent wireless local area networks may be transmitting on the same or adjacent channels to the one you have chosen.

In order to change the channel of your wireless router, log onto it with your user name and password. Then change the channel to meet your needs. A first step may include using a laptop computer to search for access points in your surroundings and then randomly choosing a channel that is not already being used. Information about the channels of other wireless local area networks can often be found by searching for such networks, which normally takes place by activating 'find networks' or the like. All of the access points in your surroundings will then be listed on your computer screen (regardless of the channel that they broadcast on) and detailed information is usually presented for each access point; for example, the channel that is used, encryption, name, signal strength, etc. It will be clear if the new channel is working well or not as the computer will not make contact with the access point if it is not working. There is often an indication of the signal strength and link quality of the software for the wireless network cards that are, for example, built into laptop computers.

Changing channels reduces the risk of radio interference. See Section 3.3 for more information about interference in wireless local area networks.

6.2 Security advice for users of public wireless networks

PTS provides some pieces of advice for users of public wireless networks. Users of such networks should bear in mind that data is usually not encrypted in these networks. For this reason, be cautious with the information that you send and

receive. Using the Internet for surfing and reading information is safe provided your computer is equipped with an up-to-date operating system, firewall and antivirus program. Do not use your credit card number or important login details when on a public wireless network unless there is an https:// or a VPN solution. The general advice provided in the next section, 6.3, should also be taken into consideration for public wireless networks. See Sections 3.1 to 3.3 for more information about different risks.

6.2.1 Assume that all communication is unprotected and use a secure connection when dealing with sensitive information

Assume that all communication is unprotected and unencrypted in public wireless networks and protect yourself by using a secure connection when dealing with sensitive information. Only communicate sensitive information when using websites with protected connections, such as https, or use a VPN solution.

Avoid sending sensitive information such as credit card numbers, user names and passwords, personal details, sensitive files or e-mail messages containing such information if you are not using an encrypted tunnel (VPN) or do not have an https:// connection connected to the server or website that you are communicating with.

When using critical services on the Internet that make use of your important passwords to, for example, Internet banks, tax authorities, etc., or, for example, your credit card when buying goods or services online, it is important to ensure that the Internet connection is an https:// connection; that is, a secure connection. An encrypted connection has then been established between the server and your computer, and the content that is transmitted is protected. You can see whether you have a secure Internet connection by the beginning of the address field of your web browser stating https:// instead of http:// and when a padlock is displayed in the web browser.

A VPN solution is a secure connection between two points and is often used in corporate solutions so that employees can access internal company information; for example, the intranet and company e-mail. An encrypted tunnel (VPN) is created by a special program and is usually installed by the employer, but can also be installed/downloaded by the user.

If you use your employer's computer, it is important for data security reasons that you comply with your company's regulatory framework for data security. In addition to VPN solutions, it is also possible to encrypt e-mail. However, note that if you have not established a VPN tunnel before encrypting your e-mail messages, all login details for your e-mail will be communicated without any protection and will be unencrypted.

Using an encrypted tunnel (VPN) or secure Internet connection in the form of https will establish a secure connection to a server or website and you can then send sensitive information. You should also pay attention to the original address of a website. See Section 3.1 for more information about risks.

6.2.2 Ensure that you do not unwittingly communicate with the outside world

Ensure that you do not unwittingly communicate with the outside world. Some computers' operating systems connect to the outside world without users taking any action or being able to discover it easily. Examples of this include functions such as ad hoc, i.e. establishing random, small wireless local area networks between laptop computers, handheld computers and smartphones using WLAN technology, depending on what is available in the surrounding area. Disconnect the ad hoc function so that you are not unwittingly communicating with the outside world.

You should also be careful with the file sharing function on your computer. This function enables users to share files with others in a network. It is usually used in local environments such as at home or at work. However, if it is not disconnected, this could be a way in for parties who wish to access the user's computer.

Ensuring that you are not unwittingly communicating with the outside world reduces the risk of unauthorised parties gaining access to your sensitive information. See Section 3.1 for more information about risks.

6.2.3 Be aware of false access points

Be aware of false access points and only connect to access points that you consider to be genuine. If you discover the same name being used by two or more wireless local area networks (i.e. the same SSID) in the same location, such as at a café or train station, do not connect to it if you are not entirely sure of the name of the network and if it does not offer a secure connection in the form of <https://> when logging in. If the service provider offers an <https://-connection> and the web address to the service provider appears to be correct, it has established a secure connection between your computer and the login server so that you can, for example, safely pay for the service.

If you are unsure of the networks that should be available and their names, ask the owners of the wireless local area networks, or alternatively the owner of the café, restaurant, hotel or the like.

Being aware of false access points reduces the risk of unauthorised parties gaining access to your sensitive information. See Section 3.1 for more information about risks.

6.2.4 Be aware of social factors

Be aware of different social factors; for example, if someone attempts to read over your shoulder. This particularly applies when logging onto e-services and when stating your user name and password. As a main rule, never leave your laptop computer unattended. If you have to leave your computer for a short period of time, lock it securely using a cable or in some other way and lock down the computer so that it cannot be used.

Being aware of social factors reduces the risk of someone gaining unauthorised access to your sensitive information.

6.3 General security advice when using the Internet

PTS also provides Internet users with general advice so that they can achieve good basic security in their computer environments regardless of whether they have a wired or wireless connection to the Internet. First and foremost, Internet users should protect their computers and the data on them before connecting to the Internet.

6.3.1 Ensure that you have an up-to-date firewall, antivirus program and operating system

Ensure that your computer has an up-to-date firewall, antivirus program and operating system. This lays the foundation for good security when surfing on the Internet.

The operating system is usually updated automatically and users receive a message when updates are being downloaded and installed once these are authorised. Updates to firewall and antivirus programs take place in different ways. Some take place automatically, whereas others require users to actively search for updates.

Up-to-date operating systems, firewalls and antivirus programs can keep unexpected and malicious events (malware) away from your computer. Such programs can make your computer turn itself off uncontrollably, or copy, modify or delete data on your computer.

6.3.2 Choose and use strong passwords

Choose and use strong passwords. A password contributes to the strength of the level of encryption for your private wireless network. This password should contain a combination of characters consisting of at least eight characters, should not be the name of a family member nor a word that exists in a dictionary or the like, since there are programs that test passwords against dictionaries. The password should contain a mixture of capital and lower case letters, numbers and other characters such as *,@, }, etc.

PTS's web service, *Testa lösenord* [Test your password] (<https://www.testalosenord.se/>) gives users the opportunity to test different combinations of characters to determine whether they would be strong or weak if used as passwords. Do not use this service for testing passwords that you already use or for creating new passwords that you intend to use. Always manage passwords carefully and only use them when you want access to the service for which they are intended.

Using a strong password makes it more difficult for unauthorised parties to gain access to your computer, your network and your data.

7 Positions adopted focussing on continued work

Summary of Chapter 7

Service providers shall inform users about the level of security of their network and provide users with recommendations.

Suppliers of equipment for wireless local area networks should facilitate security measures through improved factory settings in new equipment and improved user interfaces.

Rules and information concerning the notification obligation under the Electronic Communications Act may be clarified in the light of new business models.

Users of public wireless networks should request improved security.

PTS will continue to monitor developments and provide information about security in wireless local area networks.

This chapter describes the positions adopted by PTS on the part of public and private wireless networks with the aim of improving security.

7.1 Service providers shall inform users about the level of security of the network and provide users with recommendations

Service providers shall provide users of public wireless networks with clear information about the level of security offered by the communication and provide users with recommendations about how they should use their networks, which are usually unencrypted.

PTS finds it unsatisfactory that service providers do not provide users with clear information about the existing level of security in their public wireless networks. Service providers have certain obligations ensuing from the notification obligation under EkomL; see Section 7.3. Currently, only a small number of service providers offer information about the level of security that prevails in their networks, but in order to make use of this information, users must actively search for the information themselves on the service provider's website; see Section 4.3 for more information.

7.2 Suppliers of equipment for wireless local area networks should facilitate security measures through improved factory settings and better user interfaces

Suppliers of equipment for private wireless networks should facilitate security measures through improved factory settings in new equipment and better user interfaces for changing settings in order to increase the level of security.

PTS considers that there is one possibility for suppliers of equipment for private wireless networks to increase the level of security in wireless networks. This can be done by supplying the equipment with better basic configurations. For example, the equipment can be supplied with encryption activated and with a unique password included with the wireless router. This is already being done by at least one broadband provider. Furthermore, it is possible for suppliers of equipment for wireless networks to further develop user interfaces and thus make it easier for users/network owners to administer and change the settings of their wireless networks.

7.3 Rules and information concerning the notification obligation under the Electronic Communications Act may be clarified in the light of new business models

Rules and information concerning the notification obligation under the Electronic Communications Act (2003:389) (EkomL) may need to be clarified in the light of new business models that are developing. PTS has observed that the new types of stakeholder and business model emerging in the market increase the need to further clarify which parties are encompassed by the notification obligation and thus also the requirements associated with the notification obligation. See Section 2.8 and Appendix 3 for more information about the obligations ensuing from EkomL.

7.4 Users of public wireless networks should request improved security

PTS considers that it is possible for users of public wireless networks to request improved security to a greater extent and thus drive forward the development of security solutions in these networks.

Users still show a relatively low level of interest in the security aspects of public wireless networks. It is likely that the main reason for this is because the market is relatively new. To date, those who seek greater security are usually corporate users, who largely utilise the company's own VPN solutions and can thus safely use wireless local area networks.

The main factors still driving the development of the public wireless network market are coverage, price, easy connection and management, as well as services, mainly capacity (transmission rate and range), but also content services. See Section 4.5 for more information about experiences gathered related to security in public wireless networks.

7.5 PTS will continue to provide information about security in wireless local area networks

PTS assesses that it will be some time before security becomes a priority for many users. For this reason, it is important for PTS to continue monitoring developments and providing users with information about the existing level of security in the market for wireless local area networks. For example, this includes

producing advice on how users can protect themselves through technical solutions and configurations in addition to recommendations for network behaviour that enhance security in wireless local area networks.

For current advice from PTS, see Chapter 6 and monitor the situation on PTS's website about Internet security (<http://www.pts.se/internetsakerhet/Sidor/startside.asp>).

Bibliography

Electronic Communications Act (2003:389) (EkomL)

Government use of wireless broadband, Department of Communications, Information Technology and the Arts, 2004 (Australia)

Guidance on the 'Public Proclamation concerning the exchange of registers and storage of telecommunications traffic data within electronic communications networks and electronic communications services' (Data Logging Proclamation), referring to Section 786, paragraphs 4 and 7 of the Data Logging Proclamation no. 910, 27 September 2005), Danish Ministry of Justice, 2006

Information security guide for electronic service providers, LUOTI (Finland), 2006

Information security in wireless networks, LUOTI (Finland), 2006

Information security threats and solutions in the mobile world, VTT Research (Finland), 2005

NISCC Technical Note 04/02: The Security of 802.11 Wireless Networks, 2002, Centre for Protection of National Infrastructure (CPNI) (United Kingdom)

Om trådlösa nätverk, PTS information brochure [reference at end of 1.5 and Appendix 5, Section 1 gives *Om lokala trådlösa nätverk* – About wireless local area networks?]

Our demand for electronic information – a Survey of Individuals, National Post and Telecom Agency, 2006 (PTS ER-2006:47)

Personal Data Act (1988 [this should be 1998];204) (PuL)

PTS Policy concerning IP-based telephony vis-à-vis a number of concrete substantive issues, National Post and Telecom Agency, 2006 (PTS-ER-2006:39)

PTS Regulations, National Post and Telecom Agency, 2005 (PTSFS 2005:8)

Public Proclamation concerning the exchange of registers and storage of telecommunications traffic data within electronic communications networks and electronic communications services (Data Logging Proclamation), referring to Section 786, paragraphs 4 and 7 of the Data Logging Proclamation no. 910, 27 September 2005), Danish Ministry of Justice, 2006

Security threats to mobile telephony. An assessment of the current situation - winter 2005/2005, National Post and Telecom Agency, 2006 (PTS-ER-2006:18)

Spyware and closely related phenomena, National Post and Telecom Agency, 2005 (PTS-ER-2005:15)

Strategy to improve Internet security in Sweden, National Post and Telecom Agency, 2006 (PTS-ER-2006:12)

Säkerhet i trådlösa nätverk [Security in wireless networks], Fredrik Olsson, 4G Media, 2006

Säkerhet i trådlösa nätverk [Security in wireless networks], preliminary study by Netlight Consulting AB on the assignment of the National Post and Telecom Agency, 2006

The Penal Code

The wireless society: an investigation of the legal situation, the security situation and security awareness when using wireless home networks, Växjö University, thesis, 2006.

Wireless LANs – design and security, Fact Sheet 81, Australian Communications and Media Authority, 2003

Wireless networks, WLAN - A technical market report, National Post and Telecom Agency, 2004 (PTS-ER-2004:12)

Websites

PTS's website about Internet security,
<http://www.pts.se/internetsakerhet/Sidor/startside.asp>

Australia

In Australia, a report was produced by the Australian Government Department of Communications, Information Technology and the Arts (DTCIA) containing guidelines for suitable measures on how central government should use wireless networks, <http://www.dcita.gov.au/>

The Australian Communications and Media Authority is the Australian counterpart to PTS, <http://www.acma.gov.au/web/homepage//pc=home>

Canada

Strategis, the official government website for corporate and consumer issues, <http://strategis.ic.gc.ca/engdoc/main.html>

Direct link to advice for improving security when using wireless networks, <http://www.strategis.ic.gc.ca/epic/site/dir-ect.nsf/en/uw00354e.html>

Denmark

The National IT and Telecom Agency is the Danish counterpart to PTS, <http://www.itst.dk/>

Advice from the National IT and Telecom Agency concerning protection in wireless networks, <http://www.it-borger.dk/sikkerhed/anbefalinger-det-bor-du->

gore/tradloose-netverk-og-sikkerhed/sikkerheden-i-offentlige-og-felles-tradloose-netverk

Finland

The Ministry of Communication's development programme (LUOTTI) promotes confidence in data security as regards electronic services, <http://www.luoti.fi/se/index.html>

Norway

The Norwegian Post and Telecommunications Authority (NPT) is the Norwegian counterpart to PTS, <http://www.npt.no>

The Norwegian Post and Telecommunications Authority provides security information and advice through a campaign called Nettvett ['Net sense'], <http://www.nettvett.no>

United Kingdom

In the United Kingdom, data security work is managed by a central authority called the Centre for Protection of National Infrastructure (CPNI), <http://www.cpni.gov.uk/>

Get Safe Online is a British campaign to improve security awareness among the general public. It is run by various public authorities, the police and representatives of private companies within the industry, http://www.getsafeonline.org/nqcontent.cfm?a_id=1131

United States

OnGuard Online is a website and an initiative run by a number of federal authorities and representatives within the American technology industry for informing users about security risks in connection with Internet use, <http://onguardonline.gov/wireless.html>

GetNetWise is a public service run by representatives of the Internet industry and various public interest organisations. They provide information and advice about improving Internet security, <http://security.getnetwise.org/tips/wifi>

Wi-Fi Alliance

The Wi-Fi Alliance is an industry organisation working to promote the adoption of a single worldwide-accepted standard for WLAN, <http://www.wi-fi.org/index.php>

The Wi-Fi Alliance's website about security: <http://www.wi-fi.org/searchresults.php?c=11&sp=Security&pm=pubParams>

Appendix 1 – Definitions of concepts and abbreviations used

This appendix defines the concepts and abbreviations used in this report.

1 Definitions of concepts

Access control	Verification of which client equipment should get access to a specific network.
Access point	Network device that provides clients with wireless access to a network; e.g. a wireless router.
Ad hoc network	The name for a WLAN without central flow control. Typically, this comprises a computer connected to the Internet and a number of clients sharing the Internet connection.
ARP spoofing	<p>ARP (Address Resolution Protocol) is a protocol for translating IP addresses into the correct hardware addresses, or MAC addresses, in a local network in order to forward traffic from the Internet (or a local network) to the correct computer in the local network.</p> <p>ARP spoofing means that traffic in the wireless local area network is intercepted and the data is used so that traffic intended for a certain computer is sent to another computer.</p>
Authentication	Verification of a stated identity.
Authorisation	Verification of the access rights and authorisations of an authenticated user.
Bluetooth	A wireless technology for transmitting data over short distances between different devices; for example, a telephone and a computer.
Botnet	A botnet is a network of computers infected by computer viruses and Trojan horses. These computers connect to a central control node where they receive tasks; for example, carrying out DoS attacks against interconnection points on the Internet. A botnet may consist of thousands of computers spread around the world and whose owners are unaware that their computers are infected.
Broadband modem	An (xDSL) modem where 'x' signifies different

	technologies for transmission.
Broadcast	Broadcast means that information is sent to all potential and interested recipients of the information. Typical examples include standard broadcasting including television, where all people who have selected a certain radio frequency can listen to the programme.
Channel	A frequency band can be divided into channels so that devices on the same band do not completely interfere with each other.
Crypto keys or keys	These are a sequence of characters on a number of bits that enable encryption and decryption of data with the aim of making the data sent incomprehensible to unauthorised parties.
Denial-of-Service attack (DoS attack)	A DoS attack is an overload attack against a computer system. There are three different methods of carrying out this type of attack: taking advantage of a vulnerability or weakness which causes the system's software to crash; transmitting (overloading) so much traffic that the system or application collapses; and sending so much junk traffic that legal/valid traffic is prevented from getting through.
Dynamic IP address	A dynamic IP address indicates that the IP address to the network hardware or a computer connected to a network is not static, but is allocated automatically, often by a DHCP server. DHCP servers are often found in routers.
Encryption	Encryption is used to distort data so that only those parties who are intended to read it can do so.
Encrypted tunnel	An encrypted tunnel is a secure connection set up between a client and a server; the https protocol or the VPN security solution can set up this type of tunnel.
Evil Twinning attack	An Evil Twinning attack means that a false access point has been set up at a public location using the same network name (SSID) as a public wireless network that is already well-known (the 'evil twin') so that users believe that it is a genuine network. False access points often transmit with stronger signal strength than the genuine ones so that computers connect to these. In this way, a false access point can intercept unencrypted data.

Firewall	<p>Software firewall: a program that monitors the traffic entering and leaving the computer and prevents prohibited communication.</p> <p>Hardware firewall: May be created by means of a router that filters packets before they reach the computer.</p>
Firmware	Firmware is the same thing as software programmed into hardware. Firmware can be found in computers, digital cameras and used for decoding routines in DVD and MP3 players. Firmware can sometimes be updated by downloading an update file in the equipment.
Handover	A common term within the world of mobile telephony which indicates the handover between base stations within an operator's network during an ongoing call (voice, data, etc.).
Hotspot	A hotspot is usually the same thing as a public access point.
Hot zone	A hot zone is a wireless area that is larger than a hotspot.
Infrastructure network	A WLAN with central flow control. It usually consists of a router/access point with a WLAN function and a number of clients who can reach each other and other networks via the central access point.
IP address	An IP address from the sender and an IP address from the recipient are required in order to communicate via the Internet. 'IP' stands for Internet Protocol.
IPsec	IPsec is an abbreviation of 'IP security' and is used to create permanently encrypted tunnels between two or more points on the Internet. IPsec establishes a link between two points – a tunnel – within which encrypted traffic can be transmitted while blocking people who may be trying to intercept the traffic from being able to view the content or seeing what type of traffic is being sent through the tunnel.
Linux	An operating system based on open source codes.
MAC address	A hardware address that is unique to each network card and thus each wireless device.
Malicious code	Malicious codes refer to worms, Trojans, viruses, etc., whose intention is to exploit a certain vulnerability and

	cause damage, steal data, etc.
Man-in-the Middle attack	Man-in-the-Middle is an interception attack where a device places itself between the sender and the recipient and intercepts the data. In this way, sensitive login details for important e-services can be easily intercepted by unauthorised parties.
Mesh network	A mesh network, IEEE 802.11s, consists of a number of nodes, where each node is connected to adjacent nodes to ensure redundancy and to expand network coverage. This is a further development of WLAN technology and can provide wireless coverage over large urban areas.
Mobility	In this context, mobility refers to communication, for example, a voice call or surfing on the Internet, being able to continue functioning without interruption, even when moving around. For example, this means that the technical solutions must be capable of handing over the call between different base stations without breaking the connection. This function is built into various mobile systems such as GSM and 3G.
Network card	Network cards are integrated into all computers and routers and constitute a unique ID (MAC address) for the device so that devices can communicate with each other correctly in a network.
Operating system	An operating system is a program in a computer whose purpose is to facilitate use of the computer by serving as the link between the computer's hardware and the programs run on the computer.
Protocol	A protocol is a set of rules about how two or more computer programs should communicate with each other.
Roaming	Within mobile communications, roaming means changing from one network to another. This usually occurs when a user is in a country other than the country of subscription, in which case it is known as 'international roaming'.
Router	A router is a computer or network device which connects several local computer networks together. In packet-switched networks, the router determines the next network address that the data packet is to be sent to. A packet usually goes through many routers before

	reaching its final destination.
Shared key	A crypto key which is used to provide access to a wireless network as well as encrypt traffic in a wireless network. The same key is used for all users and is consequently shared between them. A shared key is also known as a PSK, a Pre-Shared Key.
Spam	Spam is an e-mail message, often an advertisement, that the recipient has not requested in advance. It is also known as 'junk mail' and is usually more of a nuisance than a security risk, although viruses can be sent via spam.
Spyware	Spyware attempts to compile data about your habits. In most cases, it is more of a threat to the user's privacy than to the computer as such. Spyware is often downloaded together with another program without the user being aware of it or the user being realising what his or her actions imply. The program then compiles data about the user's Internet habits and sends it to external recipients.
Static IP address	Your Internet service provider will allocate you a static IP address if you have a fixed Internet connection.
Symmetric encryption	An encryption method where the same key is used for encryption and decryption.
Wireless router	A device that transmits data traffic to and from one or more computers via radio waves.
Wi-Fi Alliance	A trade organisation that produces standards for WLAN technology.

2 Explanations of abbreviations

3G	Third generation mobile telephony systems and the successor to the NMT and GSM systems. 3G, or UMTS (Universal Mobile Telecommunications System) as it is also sometimes known, enables more rapid data transmission to and from mobile telephones and other mobile terminals. The system can be used for voice, for sending and receiving graphics, still images and moving images, etc.
AES	Advanced Encryption Standard. Encryption technology that is a standard for WPA2.
ARP	Address Resolution Protocol; it translates global IP addresses to local, specific MAC addresses.
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. This is the protocol used in WPA2 and which describes key management, message integrity and encryption technology (AES).
CRC-32	Cyclic Redundancy Check (32-bit). An algorithm for checking data integrity. It is used to verify message integrity in WEP.
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance is an algorithm for granting access to the wireless access medium.
DHCP	Dynamic Host Configuration Protocol is a network protocol that enables the dynamic allocation of IP addresses to computers on a LAN. A system administrator assigns an IP address field for DHCP and each computer in the LAN has its own software so that it can automatically request an IP address from the DHCP server.
DoS	Denial-of-Service. An attack where a service is bombarded with requests, which leads to the service becoming overloaded and blocked, or disrupts signals or blocks the service in some other way.
EAP	Extensible Authentication Protocol is a universal authentication protocol. EAP is usually used in wireless local area networks. The WPA and WPA2 standards have recently implemented five EAP methods as their authentication mechanisms. The EAP methods EAP-TLS, EAP-SIM, EAP-AKA, EAP-TTLS and LEAP are

	the most common authentication methods.
EkomL	The Electronic Communications Act (2003:389)
EIRP	Equivalent Isotropically Radiated Power is a comparative measurement that indicates the power required by a transmitter in order to radiate power evenly in all directions as in the main lobe. The more the antenna concentrates the energy radiated by the transmitter to the main lobe, the higher the EIRP.
GSM	Global System for Mobile communications, which is the most popular standard for mobile telephony. This standard has become popular since it enables efficient international roaming between operators.
http	Hypertext Transfer Protocol is a protocol for transferring and displaying web pages on the Internet.
HTTPS	Hypertext Transport Protocol Secure is used for the encrypted transport of data. A certificate from a third party is required for a web server to be deemed trustworthy. This certificate is installed on the web server and verifies that the server is a trusted server.
IEEE	Institute of Electrical and Electronics Engineers. A professional organisation that develops many of the technologies standardised within ITU.
IEEE 802.11a	An older standard for wireless local area networks. It uses the 2.4 GHz and 5 GHz bands.
IEEE 802.11b	A standard for transmission in wireless local area networks. It uses the 2.4 GHz band and has a maximum transmission rate of 11 Mbit per second.
IEEE 802.11e	Expansion of the IEEE 802.11 standards, including functionality for Quality of Service.
IEEE 802.11g	A standard for transmission in wireless local area networks. It uses the 2.4 GHz band and has a maximum transmission rate of 54 Mbit per second.
IEEE 802.11i	Security standard for wireless local area networks. Partially implemented by WPA and fully implemented by WPA2.
IEEE 802.11n	Future standard for transmission in wireless local area networks. It uses the 2.4 GHz and 5 GHz bands and has a maximum transmission rate of 54 Mbit per

	second. Based on MIMO technology.
IEEE 802.11p	Future standard for mobile wireless local area networks. It uses the licensed 5.9 GHz band and can achieve rates of up to 6 Mbit per second for average distances of up to 300 metres.
IEEE 802.11s	Future standard for wireless mesh networks.
IEEE 802.11x	Collective term for the standards within the IEEE 802.11 framework, including IEEE 802.11a/b/e/g/i/n/p/s.
IEEE 802.16e	It expands IEEE 802.16 to enable functions for mobility, such as handover and QoS.
IEEE 802.1X	Protocol for user authentication intended for use in wireless local area networks.
ISP	Internet Service Provider
LAN	Local Area Network. A general term meaning 'local network'.
MAC	Media Access Control. An algorithm to determine whether or when a device may transmit via a network.
MIMO	Multiple Input Multiple Output. Technology within IEEE 802.11n that uses several antennae instead of one in order to increase the transmission rate.
PSK	Pre-Shared Key, see Shared key.
PTS	The National Post and Telecom Agency (PTS) is the Swedish authority that monitors the areas of electronic communications and postal services. The concept 'electronic communications' encompasses telecommunications, IT and radio.
PuL	Personal Data Act
QoS	Quality of Service. Mechanisms to ensure quality in a network relating to bandwidth, delay and variations in delay.
RADIUS	Remote Authentication Dial-In User Services is often used for big authentication servers in order to authenticate users of a network.
RC4	An encryption algorithm used in WEP and WPA. WEP

	uses a key length of 40 bits and WPA uses a key length of 104 bits.
RFID	Radio Frequency Identifier is a technology for reading and storing data at a distance from small combined radio transmitters/receivers and memories.
SSID	Service Set Identifier. An alphanumeric string that defines a specific wireless network.
SSL/TLS	Secure Socket Layer/Transport Layer Security is a method to establish a protected, encrypted connection between a website and a web browser.
USB	Universal Service Bus is a standard for transmitting data to and from a computer using a cable connection. It is commonly used for, for example, external memory devices (USB memory), MP3 players, digital cameras, etc.
VoIP	Voice over IP is a popular term for IP-based telephony. For more information about IP-based telephony, see PTS's policy concerning IP-based telephony vis-à-vis a number of concrete substantive issues (PTS-ER-2006:39)
VPN	Virtual Private Network. Common technology for establishing a secure (encrypted) link between two points in a network.
WEP	Wired Equivalent Privacy. The security standard used within the framework of the original IEEE 802.11 standard and which is common in wireless home networks. It is generally considered to be insufficiently secure.
Wi-Fi	Wi-Fi is sometimes used instead of the term WLAN. Wi-Fi is a trademark owned by the Wi-Fi Alliance, which uses the Wi-Fi term for certifying equipment.
WiMAX	Worldwide interoperability Microwave Access standardises wireless broadband over great distances. Another name for this standard is IEEE 802.16.
WLAN	Wireless Local Area Network. General term used to describe such networks.
WPA	Wi-Fi Protected Access. Standard from the Wi-Fi Alliance for security in wireless local area networks, which is based on an incomplete version of IEEE

	802.11i. WPA resolved the existing problems of WEP.
WPA2	A standard from the Wi-Fi Alliance based on IEEE 802.11i. Includes CCMP.

Appendix 2 – A technical description of wireless local area networks

Contents

1	Reading instructions	66
2	Description of the framework behind WLAN technology	66
2.1	Mesh networks comprise individual nodes which collectively establish wireless coverage over entire cities and support mobility.....	66
2.2	Summary of several standards within WLAN technology	67
3	Security solutions for wireless local area networks	67
3.1	Authentication verifies a given identity against a network.....	68
3.1.1	Authentication in large networks is performed by a central authentication server.....	68
3.1.2	Local authentication takes place using keys based on the router's password.....	68
3.1.3	Authentication using a shared key is common in simpler equipment.....	69
3.1.4	WEP: the first generation of encryption standard for wireless local area networks is easy to decrypt.....	69
3.1.5	802.11i: a standard produced to improve the security of wireless local area networks	70
3.1.6	WPA: the second generation of encryption standard is more secure than WEP, but insufficiently secure for today's market	70
3.1.7	WPA2: the third and latest generation's encryption standard is currently viewed as secure.....	71

1 Reading instructions

This appendix briefly describes the standardised framework that serves as a basis for WLAN technology and the IEEE 802.11x family. This is followed by a more detailed description of the future standard for mesh wireless networks than that contained in Chapter 2 of the report. These descriptions are followed by an illustrative table of a number of WLAN standards in Section 2.2. Authentication is also described in more detail since it is an important security solution for computer networks. Lastly, an account is provided of three security standards which were developed to improve the security of wireless local area networks.

2 Description of the framework behind WLAN technology

Wireless LAN, WLAN, Wireless Local Area Network, Wi-Fi and IEEE 802.11x are all terms for the same technology. WLAN technology uses the unlicensed 2.4 and 5 GHz frequency bands for the wireless transmission of data between computers, handheld computers, VoIP telephones and access points, etc.

IEEE 802.11x is a collective name for a number of standards from the IEEE (Institute of Electrical and Electronics Engineers), where 'x' denotes several standards within IEEE 802.11 that contribute to wireless computer communications with different functionality; for example, different data transmission rates, range, QoS requirements (Quality of Service requirements) and security. Examples of standards encompassed by the IEEE 802.11 framework include IEEE 802.11a/b/e/g/h/i/n/p/s/X. IEEE 802.11x should not be confused with IEEE 802.1X, which is a standard for new methods for improved security in WLAN. New standards within the framework of IEEE 802.11 and WLAN technology are continually being developed to drive the development and technology of WLAN forward. Section 2.1 below describes a future standard for mesh networks in more detail.

2.1 Mesh networks comprise individual nodes which collectively establish wireless coverage over entire cities and support mobility

A 'mesh network' is a further development based on WLAN technology and can provide wireless coverage over large areas of cities. The IEEE 802.11s standard is being developed and will standardise this type of wireless network. This WLAN standard also supports mobility within the network; that is, that a user can move around while being connected to the network without losing the network connection. A mesh network consists of a number of nodes, where each node is connected to adjacent nodes to ensure redundancy and expand network coverage. According to the current time schedule, the IEEE 802.11s standard will be finally published in April 2008. The transmission standards between mesh nodes are described by IEEE 802.11a/b/g/n, while IEEE 802.11s describes how important functions such as routing, security and QoS should be achieved in a mesh network. Since most of the major mesh equipment suppliers are involved in the

standardisation work, today's mesh solutions are often directed at the standard, but there is no guarantee that there will be compatibility between the different suppliers. One service provider located in Sweden has introduced at least one such network to a city and intends to increase the number of mesh networks.

2.2 Summary of several standards within WLAN technology

Two summaries of WLAN standards are presented below. The first table indicates the year, frequency band, data transmission rate and range of the four most common types of WLAN standard. The second table shows the year, frequency band and purpose for which the standard was primarily developed.

Development of WLAN standards for data transmission rates

Standard	Year	Frequency band	Rate	Range
802.11a	1999	5 GHz	54 Mbit/s	Approx. 30m
802.11b	1999	2.4 GHz	11 Mbit/s	Approx. 100m
802.11g	2003	2.4 GHz	54 Mbit/s	Approx. 60m
802.11n	2007/2008	2.4 and 5 GHz	100 Mbit/s	Approx. 70m

Development of WLAN standards for different purposes

Standard	Year	Frequency band	Description
802.11e	2005	5 GHz	Management of QoS requirements
802.11i	2004	2.4 GHz	Improved security
802.11s	2007/2008	2.4 GHz	Mesh networks

3 Security solutions for wireless local area networks

A number of different protocols, technologies and security mechanisms are needed to ensure security in wireless local area networks. Computer networks and computer systems often need to be able to verify a given identity and thereby only provide authorised users with access to information and programs. As previously stated in the report, examples of security mechanisms for use of a computer network (wired or wireless) include authentication and encryption; see also Section 2.5 of the report. Some encryption methods use the password from the

authentication (the logging in) of a person who wishes to use a network or computer system, for which reason authentication or encryption are sometimes closely linked. The protocols and standardised security solutions currently developed and used in wireless local area networks are relatively new and a number of vulnerabilities have appeared over time. An overview of the technically standardised security solutions for authentication and encryption is provided below.

3.1 Authentication verifies a given identity against a network

Authentication is a security solution in a computer network which checks a given identity to verify that the user is who he/she claims to be. It is also used to identify who has access to the network during the period in which the user is logged in. Authentication takes place using a user name and password. The password is often used when encrypting data transmitted in the wireless local area network; i.e. if the network uses an encryption standard.

3.1.1 Authentication in large networks is performed by a central authentication server

Authentication in large networks is often performed with a special server; for example, using the RADIUS protocol, which transmits login data about users to a RADIUS server. A RADIUS server checks who is logging onto the network (authentication), what the user may or may not do on the network (authorisation) and manages payment information. An authentication server keeps an account for each network user. This type of authentication is not supported by systems using the WEP encryption method. Many networks, such as those from Internet service providers offering fixed connections, require some type of logging in when the user is to use the network or when a user wishes to log onto a wireless public network using WLAN technology. A RADIUS server checks that the data about the user is correct before the user is connected to the network using, for example, EAP (Extensible Authentication Protocol), which is commonly used for wireless local area networks.

3.1.2 Local authentication takes place using keys based on the router's password

Small wireless local area networks seldom offer access to an authentication server and, as regards the access points that can be purchased in the trade, they rarely have such functionality built in. This functionality is also not specified for equipment developed prior to 2003.

The most common procedure for authenticating users in wireless local area networks is the use of crypto keys, usually in the form of a password stored in a wireless router. More advanced products enable the storage of several user accounts and can in this way function somewhat as an authentication server.

Local authentication works similarly to RADIUS authentication, with the exception that the access point takes over the tasks of the authentication server. Such implementations are usually simpler and often less secure than an

authentication server due to the limited capacity and other restrictions of the access point.

3.1.3 Authentication using a shared key is common in simpler equipment

In many cases, and above all in simpler equipment, all users use the same shared key. This is usually called a 'pre-shared key' (PSK). When using a shared key, users cannot be authenticated in the true sense of the word; usually it is only verified that a user knows of the shared key and, on that basis, is granted access to the network. When access has been granted, the same key is used to encrypt traffic in the network. Everyone using the shared key has the same access to the network and this key should consequently only be assigned to trusted users.

Shared keys do not actually authenticate users. If a key has been saved in the client's equipment, which is relatively common, the key and access to the network will be linked to the equipment. This means that the theft of this equipment will provide access to the wireless local area network.

In a nutshell, authentication using a crypto key means that a terminal wanting access to the network sends a request to the access point. The access point sends out an encrypted message (a 'challenge'), which the terminal can only respond to if it has the correct password and is able to decrypt the message. When the terminal has responded, the access point will grant the terminal access. There are specific procedures for this exchange depending on the encryption standard used.

3.1.4 WEP: the first generation of encryption standard for wireless local area networks is easy to decrypt

The original security standard for wireless local area networks, IEEE 802.11, states that WEP (Wired Equivalent Protection) is the technology to be used for encrypted transmissions and joint authentication in wireless local area networks. The intention of introducing WEP was to achieve a level of security equivalent to that of wired networks; something, however, that was not achieved. Shortly after the specification had been completed and devices entered the market, it was demonstrated that WEP had a number of serious inadequacies making it insufficiently secure for wireless communication.

WEP uses the RC4 encryption algorithm. This is a symmetric encryption algorithm that uses a 40-bit key with a 24-bit initialisation vector in WEP. 40-bit RC4 encryption is not currently viewed as being particularly secure.

The most significant inadequacies identified in WEP (besides the fact that 40-bit RC4 encryption is not particularly strong) were the following: firstly, that the initialisation vector for encryption is too small and is reused after relatively small amounts of traffic, which means that the key can be found quickly; secondly, the algorithm (CRC32) for checking the integrity of data packets was insufficient and allowed attackers to modify the packets intercepted; thirdly, there was a lack of protection against replay attacks, so that an encrypted packet sent in the network could be recorded by an attacker and be played back later to trick devices in the network to respond to the message.

All of these inadequacies made WEP vulnerable to attacks. By monitoring WEP-encrypted traffic, an attacker can at best receive the encryption key within a few minutes. A user with basic technical skills can attack and gain access to a network protected by WEP using an ordinary computer, a network card for wireless local area networks and software that is generally available.

3.1.5 802.11i: a standard produced to improve the security of wireless local area networks

Since the security mechanisms of previous IEEE specifications were identified as inadequate, it was concluded that an update of the standard was needed. IEEE 802.11i is a modification of the original IEEE 802.11 specification from 1999. IEEE 802.11i specifies new technologies for security in wireless local area networks.

WLAN is based on IEEE 802.11i and uses a framework and protocol for authentication called Extensible Authentication Protocol (EAP). EAP is a flexible framework supporting many different types of authentication. Common types include simple passwords, single-use passwords, RADIUS authentication, etc. In wireless local area networks, EAP is extended to include an additional step where key exchange takes place. The original version of EAP only used one simple message for this, but this solution has proven to be vulnerable to a Man-in-the-Middle attack (see Section 3.1 of the report). The use of EAP enables IEEE 802.11i to support many different authentication mechanisms with various levels of security. EAP makes it possible to implement very strong authentication within the standard, but does not guarantee this.

3.1.6 WPA: the second generation of encryption standard is more secure than WEP, but insufficiently secure for today's market

The Wi-Fi Alliance developed a system called WPA (Wireless Protected Access) to rectify the vulnerabilities of WEP. WPA is based on the IEEE standard, IEEE 802.11i, but the aim was to improve security before the IEEE standardisation work was finished; this is why WPA does not fully comply with the IEEE 802.11i standard. Furthermore, the Wi-Fi Alliance wanted WPA to function with old equipment by using software updates, for which reason WPA could not implement fundamental differences from the previous standard.

WPA uses the same type of encryption algorithm as WEP, but also includes many add-ons in order to rectify the inadequacies of WEP; for example, longer encryption keys and initialisation vectors, new algorithms for packet integrity and functionality for key exchange for each packet sent. WPA is generally regarded to be much more secure than WEP, but weak passwords used to protect a wireless network using WPA makes WPA vulnerable. There is currently software available that can find shared WPA keys assuming that the handshake between a client and an access point has been recorded. Finding the key can then be done offline, without having access to the wireless local area network. Assuming that a weak password has been chosen, it is very probable that the key can be found, whereas a random password cannot generally be bypassed without considerable resources.

3.1.7 WPA2: the third and latest generation's encryption standard is currently viewed as secure

WPA2 is an additional certification from the Wi-Fi Alliance which was ready in 2006. It implements all of the obligatory components of IEEE 802.11i. A WPA2-certified product largely implements the same functionality as WPA, but besides the functions present in WPA, WPA2 also includes support for a new encryption protocol called CCMP. CCMP stands for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol Algorithm. It is based on AES (Advanced Encryption Standard), an algorithm standard that is viewed as very secure. The US Government specifies that AES with long keys (192 bits or more) may be used to protect the most sensitive classified documents, which are classified as 'Top Secret'. As of 13 March 2006, the Wi-Fi Alliance requires that all new devices support WPA2 in order to receive Wi-Fi certification.

Equipment sold today usually supports both WEP and WPA; many new devices also implement WPA2. Implementing WPA is usually a matter of developing new software and drivers for existing equipment, whereas WPA2 (more specifically CCMP) requires new hardware. It is only possible to use one of these standards in the same network at the same time. Consequently, it is not possible to use WPA devices and WEP devices at the same time. In this way, the same level of security is achieved throughout the wireless local area network, even if it means a low level of security; for example, due to a device that only supports WEP.

WPA2 and IEEE 802.11i are regarded as very secure. There are currently no known methods for attacking WPA2 besides pure DoS attacks (Denial-of-Service) and using interfering transmitters, which all networks are vulnerable to regardless of encryption technology.

Appendix 3 – Legal implications of the regulatory framework pertaining to wireless local area networks

Contents

1	Introduction	74
2	Notification obligation under EkomL.....	74
3	Important obligations ensuing from notification.....	74
4	The Personal Data Act regulates the processing of personal data where processing is not specifically regulated by EkomL	76
5	Different types of market stakeholder	77
5.1	Private users sharing access.....	77
5.2	Private users as part of a larger network with one key stakeholder.....	78
5.3	Traditional service providers: hotspots.....	79

1 Introduction

A description is provided below of some of the most important regulations that apply in conjunction with the provision of electronic communications networks and services via wireless connections. This section is not intended as a complete account of all obligations ensuing from the Electronic Communications Act (2003:389) (EkomL), but focuses on regulations describing the notification obligation, operating reliability and the protection of privacy. A more detailed description of the provisions of EkomL relating to Internet service providers can be found in PTS's report, 'The Internet and Electronic Communications Act', PTS-ER-2003:36.

2 Notification obligation under EkomL

Public electronic communications services offered to end users in Sweden can only be provided following the service providers' notification to PTS. An electronic communications service is defined as a service that is normally provided for payment and which completely or mainly comprises the transmission of signals within electronic communications networks. If a service is to be viewed as constituting an electronic communications service under EkomL, PTS's interpretation is that the service provider must in some way maintain control over some part of the transmission, either physically or legally (through ownership or an agreement). If the transmission of signals takes place via a communications network and/or a communications service that is completely independent of the service provider, (which thus has no legal possibility to affect the transmission conditions, for example, transmission capacity and quality), the service is not considered to be encompassed by EkomL's definition of an electronic communications service and is consequently not subject to the notification obligation. Networks that are entirely provided for non-commercial use are not subject to the notification obligation. However, compensation need not actually be payable for a network to be considered to be provided on a commercial basis; for this reason, for example, networks provided according to the principles of cost allocation may be subject to the notification obligation.

3 Important obligations ensuing from notification

The most important obligations ensuing from Chapter 6, Sections 5-7 include the fact that traffic data relating to users who are natural persons or relating to subscribers and which is processed and stored by the party that conducts operations subject to the notification obligation must be eradicated or prevented from being identifiable when it is no longer necessary for transmitting an electronic message. Furthermore, it is stated that traffic data may also be processed for marketing purposes if the subscriber has consented to this. Processing of traffic data may only be conducted by those who have been given the assignment by the party that conducts operations that are subject to a notification obligation, to attend to invoicing, traffic control, customer inquiries, marketing or the provision of other services where the data is needed. The processing shall be limited to that which is necessary for the operation.

According to Chapter 5, Section 6a of EkomL, a party providing public communications networks or public electronic communications services shall ensure that the operation satisfies reasonable demands for good function and technical security and also for sustainability and accessibility in the case of extraordinary events during peacetime. This provision consequently encompasses all market stakeholders providing public communications networks or public electronic communications services, regardless of technology. Through general advice, PTS clarifies how the public authority considers that the requirements of the provision should be satisfied. For example, PTS considers that service providers should carry out continuous and systematic security work and conduct risk analyses as well as manage the risks identified. In particular, service providers should plan for dealing with interference and disruptions to the electricity supply and connection routes to important functions, as well as interference and disruptions affecting their capacity to function.

According to the provisions of Chapter 6, Section 3 of EkomL, a party that provides a public electronic communications service shall implement appropriate measures to ensure that the data processed is protected. A party that provides a public communications network shall implement those measures that are necessary to maintain such protection within the network. These measures shall be intended to ensure a level of security that, taking into account the available technology and costs for the implementation of the measures, is adapted to the risk to infringement of privacy. The protection referred to is protection against wiretapping and similar acts to undermine privacy as opposed to the operational and functional security and reliability regulated in Chapter 5, Section 6a; see above. As stated, this obligation varies between a party providing a service and a party providing a communications network because the party responsible for the communications service may be said to have a more fundamental responsibility, as the market stakeholder directly processes the electronic communications, whereas the provider of the communications network only supplies the transmission route. The provision is binding and consequently may not be excluded through an agreement.

If the service provider affected has achieved the level of security required as stated in Chapter 6, Section 3 of EkomL, but it is considered that a risk still exists when using a certain form of electronic communications, the service provider is responsible for informing users about such risk and also, when applicable, how such risk may be rectified and the approximate cost of such rectification. This obligation follows from Chapter 6, Section 4 of EkomL and, as opposed to Chapter 6, Section 3, only applies to parties providing a public electronic communications service. This obligation should, for example, mean that Internet service providers in certain cases must provide information about a service and the risks associated therewith.

Chapter 6, Section 17 lays down prohibitions against wiretapping. This rule basically means a complete prohibition against making use of or in some other way processing data in an electronic message that is transmitted in a public communications network or through a public electronic communications service, or traffic data that is associated with such message, unless the user has consented

to the processing. The prohibition is associated with certain exemptions which enable processing in the form of automatic storage and caching.

There is also an exemption for parties who with the use of a radio receiver wiretap a message conveyed by radio that is not intended for this party or for the public. This exemption is justified by the fact that each individual party has the right to own a radio receiver and that it would not be advisable to impose a penalty on the wiretapping. In the *travaux préparatoires* to earlier legislation, it is considered that the air waves are free and that everyone may consequently monitor what is conveyed by radio. However, under the provision of Chapter 6, Section 23 of EkomL, it is prohibited for unauthorised parties to forward the content of such wiretapped communication.

In conclusion, Chapter 6, Section 19 of EkomL imposes an obligation on the party providing a public communications network or services within such a network which comprise a public telephony service to a fixed or mobile network termination point to conduct its operation so a decision on secret wiretapping or secret telesurveillance can be implemented and so that the implementation is not disclosed. As regards the telephony service to a fixed network termination point, this should allow the transmission of local, national and international calls, telefax and data communications with a particular specified minimum data rate which allows functional access to the Internet.

Furthermore, the content of and information about telecommunications messages that are wiretapped or under surveillance shall be made available so that the information can be handled simply. PTS can issue more detailed regulations pertaining to the fulfilment of the requirements of the provision. In individual cases, PTS may also allow exemptions from the requirements. PTS has not issued any regulations within the area.

4 The Personal Data Act regulates the processing of personal data where processing is not specifically regulated by EkomL

It follows from Chapter 6, Section 2 of EkomL as regards the processing of personal data in connection with the provision of electronic communications networks, electronic communications services and subscriber directory services that the Personal Data Act (1988:204) (PuL) applies, unless otherwise prescribed by EkomL.

PuL contains a number of provisions aimed at protecting persons from having their privacy violated through the processing of personal data. PuL applies to all processing of personal data which is carried out wholly or partially using computers. PuL contains basic requirements that apply to all processing of personal data. Personal data may, for instance, only be compiled for specific, expressly stated and justified purposes. Data compiled for a certain purpose may not be processed later for some purpose which is incompatible with the original one. More data may not be processed than that necessary considering the purposes. In addition, personal data that is processed must be correct and current,

if necessary, and must not be stored for a longer period of time than that necessary considering the purposes of the processing. PuL contains rules for when the processing of personal data is permitted. As a main rule, personal data may only be processed when registered parties have given their consent. Without such consent, data may only be processed when the processing is necessary for some of the aims stated in the Act. Since 1 January 2007, certain changes to PuL apply which aim to facilitate routine processing of personal data which does not normally entail any risk of a violation of the privacy of the registered party. For undertakings, this means that the processing of personal data in an unstructured form carried out by companies does not need to comply with the processing rules contained in PuL. PuL's processing rules still apply if this involves personal data that is included or is intended to be included in a more advanced system.

PuL also contains restrictions on the processing of sensitive personal data, information concerning offences, etc., and information about personal identity numbers. It also contains provisions concerning, among other things, information to registered parties, about correction of records and about IT security. Persons in charge of personal data are obliged to notify the Data Inspection Board of their processing of personal data. The main rule is that the Data Inspection Board must be notified of all individual processing of personal data. However, there are exemptions from this provision. In certain cases, notification may be replaced by a list drawn up and compiled by the person in charge of personal data. PuL contains provisions about penalties, fines or imprisonment for a maximum of six months for those breaching certain provisions of the Act. If the offence is grave, the penalty is imprisonment for a maximum of two years. No penalties are imposed for minor cases. A person in charge of personal information who processes personal data in contravention of PuL may be liable to pay damages to the registered person and be sentenced to compensate her or him for damage and violation of privacy caused by the unlawful processing.

The Data Inspection Board (DI) is the public authority with the supervisory role under PuL.

5 Different types of market stakeholder

Wireless Internet access is provided in many different ways. An overall legal analysis is provided below as regards some of the phenomena which may be applicable in this context.

5.1 Private users sharing access

A wireless connection may be set up by private users who intentionally or unintentionally share the broadband connection they receive through a subscription with an Internet service provider (ISP).

Private users who intentionally or unintentionally share their broadband connection are not encompassed by the rules contained in EkomL applying to the

providers of public electronic communications networks and services. In this case, transmission takes place via a communications network and/or via a communications service which in principle is completely independent of the private person who is permitting the connection. This person also has no legal possibility to affect the circumstances of the transmission. The reverse should actually apply in that a more comprehensive provision of the network capacity risks contravening the subscription agreement applying to the party 'sharing' their subscription. As stated above, air waves are free and consequently it cannot be viewed as impermissible to monitor another wireless network to which someone has not prevented automatic access. However, the party who actively prepares access to and utilises someone else's network may be guilty of an offence contravening other provisions; for example, there are rules in the Penal Code about unlawful dispossession (BrB 8:8) and unlawful use (BrB 10:7). The issue of whether or not such a procedure is an offence and which offence is relevant in this case has not yet, as far as PTS is aware, been examined by a Swedish court.

5.2 Private users as part of a larger network with one key stakeholder

A wireless connection to the Internet may also be set up through private users providing other users with access to their broadband connection, either at no charge or for a certain fee. Access assumes that registration takes place via a key stakeholder who also manages charging and compensation, etc. between the private users involved in the cooperation. One example of this is FON.

In this case, it is impossible for a user to be unaware that they are providing part of their network capacity from their Internet connection to other users – at least in those cases where it is assumed that a special router is used or special software updates are made to their own router. For example, the conditions of use for FON's service state that FON assumes that the affected users check that they have permission from their Internet service provider to share their bandwidth. Registration with FON is also required before use. Users cannot be viewed as having a legal possibility of affecting the circumstances of the transmission in this case either – even if users can to a certain extent make a decision on what proportion of the network capacity is to be reserved for their own use and what proportion should be allocated to the other parties belonging to the FON network.

Those using FON services must first conclude an agreement with FON. If the service is only intended to be used without providing one's own Internet connection, the registration that takes place means that at least the information necessary for completing a payment needs to be provided. FON accepts payment via PayPal. PayPal uses e-mail addresses as user identification in conjunction with small transactions. Customers who only intend to make payments can open a personal account. In practice, each time an account holder wishes to make a transfer, the payment takes place by PayPal debiting the relevant amount from the stated funding source of one of the account holders. This can be a bank account or a debit or credit card. Consequently, no special identity verification is made by either PayPal or FON for small transfers of this type.

The permissibility of using a certain access point is also relevant in this context. FON assumes that users who share their access have been given permission to do so. Some Internet service providers consider that such further allocation of network capacity contravenes the subscription agreements and should therefore not be permitted. In the long run, this may mean that subscribers who do so without the support of subscription terms or with other authorisation risk having their service discontinued.

5.3 Traditional service providers: hotspots

A wireless connection to the Internet can also be established by traditional service providers in the form of hotspots; cf., for example, Telia Homerun, or through new constellations of service providers. One example is the collaboration offered by Glocalnet, which means that café owners can offer their guests wireless connections. Another example is Telenor's collaboration with The Cloud.

In this case, the communications service is usually provided by traditional fixed broadband service providers. The café or shop owner involved is largely viewed as a distributor of the communications service. TeliaSonera, Telenor and other fixed broadband service providers are consequently the parties that primarily supply a public electronic communications service. They are also notified as providers of this type of service under the regulations contained in EkomL. The obligations described above apply to the operation. This means, for example, that the operation of the service provider must fulfil reasonable requirements for sound function and technical reliability. They must also take suitable measures to protect processed data and should also inform users about any remaining risks to privacy in conjunction with use and how these can be rectified, etc.

The requirement for sound function and technical reliability may be viewed in relation to the service in question and the assumptions that apply to the relevant technology. It is relatively limited in terms of range. For its Homerun service, TeliaSonera states that its range amounts to approximately 50 metres within an open area. This limited range results from the restricted output capacity that is intended to protect other transmitters/receivers from interference, which is a precondition for use being exempt from the licence obligation. The range is also affected by walls and other objects in addition to radio wave interference. It is, however, important for the service provider to inform users about restrictions to range and any limitations to capacity while providing information about the conditions of use pertaining to the service. Furthermore, it must also provide information about any inadequacies as regards the protection of processed data. If the service provider does not provide encryption, users should be informed of this and what this means while being informed of the conditions of use for the service.

Appendix 4 – An international perspective of initiatives and practical advice for improving the security in wireless local area networks

Contents

1	This appendix describes the initiatives taken by some other countries and provides examples of practical advice provided to improve security in wireless local area networks	82
2	The information and advice provided in Norway is similar to that of PTS's materials	82
3	Denmark provides advice on wireless local area networks and Danish authorities will be placing greater demands on service providers	83
4	In Finland, the Ministry of Transport and Communications promotes improved data security within wireless networks.....	84
5	The United Kingdom has a government policy for public administrative use of wireless local area networks and a campaign about data security	85
6	Federal authorities in the United States provide advice to users of wireless local area networks with additional advice also being offered by Internet service providers.....	87
7	Australian public authorities provide advice to government and the general public.....	89
8	A public authority in Canada provides advice to SMEs	90

1 This appendix describes the initiatives taken by some other countries and provides examples of practical advice provided to improve security in wireless local area networks

This appendix describes a few activities and initiatives taken in other countries by public authorities or the equivalent for the purpose of improving security in wireless local area networks. Public authorities in many countries produce recommendations and reports pertaining to threats and risks in conjunction with wireless local area networks. Most of them focus on providing advice on how users should set up their wireless local area networks in more or less the same way as PTS has done in conjunction with the brochure entitled 'About wireless local area networks'. Some also offer advice to users of public wireless networks. One problem relates to finding materials from non-English-speaking countries outside Scandinavia.

2 The information and advice provided in Norway is similar to that of PTS's materials

In Norway, information and advice to users of wireless local area networks is provided by the Norwegian counterpart to PTS, the Norwegian Post and Telecommunications Authority (PT), <http://www.npt.no>. This is mainly provided through the Nettvett portal, <http://www.nettvett.no>. Nettvett offers advice on how users can protect themselves, their private wireless networks as well as general advice about public wireless networks. The advice provided by Nettvett includes:

1. changing the standard settings for passwords and the name of the wireless device the first time that you connect to the Internet
2. activating the access control so that only the computers in your house can get access to your wireless network
3. activating encryption of the connection
4. disabling the wireless device when you are not using it
5. being aware that security is weaker when using open wireless zones and being careful about what you are doing.

There is also a section on the Nettvett website about using private wireless networks which do not belong to the user; this phenomenon is sometimes known as 'piggybacking'. A typical example is a user being able to gain access to one or more neighbours' open, private wireless networks. The point of departure of the Nettvett article is that it may be illegal to use one's neighbour's private wireless network, but that there is a lack of case-law within this area in Norway currently. They draw attention to the possible effects of piggybacking for the victim, which is reduced capacity, the risk of higher costs being incurred and a risk of demands

for damages from the Internet service provider due to a breach of contract, as sharing one's Internet access is generally in contravention of the agreement. On the other hand, Nettvett does not mention any of the risks associated with an unauthorised party abusing the identity of the open, private wireless network for illegal purposes. Nettvett does, however, draw attention to the legislation pertaining to breaches of data secrecy.

3 Denmark provides advice on wireless local area networks and Danish authorities will be placing greater demands on service providers

PTS's counterpart in Denmark, the National IT and Telecom Agency, provides information about security in private and public wireless networks and offers several pieces of advice on its website, <http://www.itst.dk/>.

The following advice is provided for the protection of wireless local area networks:

1. use encryption
2. disable the broadcast message function
3. change your standard password
4. change your SSID
5. use a firewall
6. use MAC filtering
7. check that your equipment has CE marking

ITST also provides advice to users of public wireless networks, which can be summarised as follows:

1. remember that users cannot influence the level of security in a public wireless network
2. take the same security measures as for other Internet use, such as a personal firewall and antivirus program
3. use encryption when sending sensitive information via a public wireless network.

For more information about ITST's advice, see the link <http://www.it-borger.dk/sikkerhed/anbefalinger-det-bor-du-gore/tradlose-netverk-og-sikkerhed>.

ITST is also running a campaign about data security in conjunction with several private organisations. This campaign is called '*Nettsikker nu!*' [Internet security

now!] and has been repeated annually since 2005 with different main topics each year. For more information, see the link http://www.it-borger.dk/sikkerhed/copy_of_netsikker-nu.

Compared with Sweden, greater demands will be placed on service providers in Denmark starting from 15 September 2007 when Denmark introduces new data storage directives. The Danish Ministry of Justice issued more detailed regulations pertaining to the data storage directives in September 2006 as indicated by '*Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen)*' ['Public Proclamation concerning the exchange of registers and storage of telecommunications traffic data within electronic communications networks and electronic communications services (Data Logging Proclamation)']. Guidance is also available in conjunction with this document, '*Vejledning til bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen)*' [Guidance on the 'Public Proclamation concerning the exchange of registers and storage of telecommunications traffic data within electronic communications networks and electronic communications services (Data Logging Proclamation)']. The new directives will require the provider of a public wireless network to notify where the access points are located and to register the identity of the party or parties using the network. Danish law stipulates that users may be registered; for example, in the form of MAC addresses or customer numbers. Service providers of public wireless networks must register the identity of users' equipment used for connection to the router and the IP address allocated to the users for such communication.

4 In Finland, the Ministry of Transport and Communications promotes improved data security within wireless networks

In order to promote confidence in information security in electronic services in Finland, the Ministry of Transport and Communications set up a developmental programme called LUOTI; see their website <http://www.luoti.fi/se/index.html>. This information security programme was run between 2005 and 2006. The aim of the programme was to improve data security for new electronic services functioning through many channels. Participants in the programme included various private companies, for example, within telecommunications, media and security, as well as universities, colleges, research institutes and public authorities. The main goal was to generally increase consumer confidence in e-services. A number of reports within the area were produced in the framework of the project, such as 'Information Security in Wireless Networks' and 'Information Security Threats and Solutions in a Mobile World'. The former report is a general discussion of security in wireless local area networks, i.e. WLAN, whereas the latter report discusses threats against mobile telephony and mobile terminals, among other things because they increasingly enable the placing of telephone calls via WLAN technology. These reports are written in great detail and are quite technical. Among other things, they discuss threats as well as protective measures that should be taken. The report entitled 'Information Security in Wireless

Networks' provides practical advice to users of private wireless networks. They are:

1. changing the preset user name and password for the access point.
Deactivating the possibility to carry out remote administration
2. activating encryption, such as WPA2 (or WPA if WPA2 is not available).
Choosing the most secure form of encryption possible in your network.
Even WEP is better than nothing at all. Installing secure authentication
3. changing the SSID standard to something new
4. keeping the firmware (software) of the access point up-to-date

For public wireless networks, corporate users are urged to use a VPN solution for connections to the company or organisation. All users should bear in mind that encryption on the Internet takes place at an application level via SSL/TLS (https); that is, encryption is specific to each website on the Internet.

5 The United Kingdom has a government policy for public administrative use of wireless local area networks and a campaign about data security

In the United Kingdom, data security work is managed by a public authority called the Centre for Protection of National Infrastructure (CPNI). This authority was formed following a merger of the National Infrastructure Security Co-ordination Centre (NISCC), part of MI5 (the British intelligence service), and the National Security Advice Centre (NSAC). CPNI reports to the head of MI5 and is an organisation with resources from a number of ministries and public authorities. The mission of CPNI is to provide security advice for undertakings and organisations in charge of national infrastructure. Its security advice includes security for data, individuals and physical facilities. For more information, see the CPNI website <http://www.cpni.gov.uk/default.aspx>.

One government policy contains advice concerning public administrative use of wireless local area networks; this is known as a 'technical note'. This was produced by the NISCC in May 2002, 'NISCC Technical Note 04/02". Although this government policy is five years old, it probably still applies today. The policy does not advise public administrations to use wireless local area networks with the built-in security mechanisms of IEEE 802.11 due to the weaknesses of WEP, but emphasises important technical measures if public administrations nevertheless need to use wireless local area networks. Assuming that there are strong business requirements on using wireless local area networks, the advice they offer to reduce the level of risk is as follows:

1. activate all available security functions
2. use a VPN tunnel
3. restrict the wireless local area network to the premises of the organisation

4. place the access points within the physical area of the organisation and use directional antennae to reduce the transmission of signals in unwanted directions

Specific pieces of advice about improving security:

1. change the SSID from the standard setting
2. disable the SSID broadcast function
3. disable the access point function for responding to queries by sending broadcast messages about the network
4. use MAC filtering
5. use WEP (note that this advice was written in 2002 when access to WPA was limited)
6. change the shared crypto key regularly

'Get Safe Online' is a campaign run in the United Kingdom to increase public Internet security awareness and provide advice on protection. This campaign is a collaboration between various public authorities, the police authorities and representatives from private undertakings in the industry. The target group is the general public and small undertakings. For more information, see their website http://www.getsafeonline.org/nqcontent.cfm?a_id=1.

There is a website offering advice to improve one's own private wireless network within the framework of the 'Get Safe Online' campaign:

1. use encryption. WPA2 is the best form of encryption today, but is generally only available for the very latest products. WPA-PSK is the second best form of encryption and is available for most products. If neither of these is available, for example if you are using old access points or network cards, then use WEP.
2. only use access points for wireless connection and not ad hoc, peer-to-peer networks. Access points provide more control
3. ensure that all computers in the network have a firewall (software firewall) installed
4. use public access points with caution (see below)
5. disable SSID broadcast. SSID is the name of the wireless network
6. choose an obscure SSID name. When SSID has been disabled, an obscure SSID will make it more difficult for a hacker to guess the name
7. use a strong password for gaining access to the access point

8. if your access point permits it, limit wireless access to only those hours when you are likely to use it
9. use MAC filtering. Each network card has a unique code called a MAC address. You can set up your access point so that it only provides access to the network for certain trusted MAC addresses. This will make it more difficult for unauthorised parties to carry out piggybacking.

For more details about this advice, see

http://www.getsafeonline.org/nqcontent.cfm?a_id=1151.

Get Safe Online also provides pieces of advice for users of private wireless networks. They are the following:

1. avoid using hotspots offered by parties who you are unfamiliar with or do not trust
2. if possible, use well-known service providers (here, the campaign offers examples and points out two well-known service providers)
3. disconnect the wireless local area network in your computer when it is not in use
4. disable the ad hoc mode in your computer's network card. Only allow connection to access points
5. be careful when sending sensitive information in public wireless networks, and if you do, ensure that you are using a secure website (https)
6. Use encryption. WPA is better than WEP, which in turn is better than nothing at all
7. use VPN when connecting to company networks
8. ensure that your general level of security is satisfactory, especially your firewall

For more detailed advice, see

http://www.getsafeonline.org/nqcontent.cfm?a_id=1131.

6 Federal authorities in the United States provide advice to users of wireless local area networks with additional advice being offered by Internet service providers

'OnGuard online' is a website and an initiative from a number of federal authorities and representatives from the technology industry in the US for informing users about security risks in connection with Internet use,

<http://onguardonline.gov/wireless.html>. The message from these authorities is not to assume that public wireless networks are secure. Assume that the traffic you send and receive can be read by others. The website also provides some tips about how to protect oneself when using wireless local area networks, including one piece of advice about public wireless networks (number 8). The recommendations provided are:

1. use encryption
2. use an antivirus program, an antispymware program and a firewall
3. disable broadcasting of the network's identity
4. change the network identity from the router's basic configuration
5. change your router's preset password for administration
6. only allow specified computers access to your wireless network
7. disconnect your wireless network when you know that you will not be using it
8. do not assume that public hotspots are secure

GetNetWise is another source of information and advice in the United States. GetNetWise is a public service provided by representatives of the Internet industry and various interest organisations. For more information, see <http://www.getnetwise.org/about/>. GetNetWise offers the following checklist and advice:

1. Does your hotspot contravene your agreement with your Internet service provider? (This applies to those keeping their private wireless networks open to everyone, a situation that may be viewed as a private person setting up their own hotspot.)
2. Are your computer and network secure? This particularly applies to the use of strong passwords
3. Have you changed the password of your access point from the standard password supplied with new equipment?
4. Do not send out broadcast messages using the network name (SSID)
5. Use encryption
6. Configure your access point so that it only permits your MAC addresses (i.e. use MAC filtering)

7. Do not send sensitive information in wireless local area networks if you do not know that it is secure; i.e., an https connection
8. Use a VPN solution to ensure security for all traffic in wireless local area networks. (This advice is especially directed at users who connect to their workplace or send information that is related to work, such as files and e-mail.)

7 Australian public authorities provide advice to government and the general public

A number of projects have been financed by the Australian Government through the Department of Communications, Information Technology and the Arts (DTCIA), <http://www.dcita.gov.au/>. An extensive report was produced on the assignment of the DTCIA entitled 'Government use of wireless broadband'. This report reviews the various threats to security and privacy when using wireless local area networks. Different protective measures are also proposed in conjunction with this, termed as 'best practices'.

1. Ensure that the access point does not send out the network name (SSID)
2. Ensure that the crypto keys are configured for dynamic replacement. Static keys can be decrypted through monitoring and interception of wireless communications
3. Set up and maintain a firewall between the access point and the internal network
4. Ensure that the equipment in the wireless network has been correctly set up. WPA2 is the latest crypto standard. The best practice security standard recommends further encryption of communication signals by using VPN
5. Implement appropriate mechanisms for authentication, such as authentication servers (RADIUS), single-use passwords or digital certificates
6. The transmitter's signal strength should be configured so it covers the area needed. Make sure that the distance and signal strength of the transmitter signal from the access point are suitable and do not extend further than necessary beyond the area requiring coverage. This can be done through careful placement of the antenna and by adjusting the signal strength, which reduces the potential of an attacker to receive or intercept wireless signals.

The Australian Communications and Media Authority (ACMA) is the regulatory authority for broadcasting, the Internet, radio communications and telecommunications, which means that it is largely a counterpart to PTS. ACMA has issued a factsheet about security in wireless local area networks directed at

consumers and service providers. ACMA starts by stating that there is no fundamental difference between setting up a wireless network and setting up a wired network. The advice provided by ACMA indicates that the following areas need to be borne in mind:

1. identifying the user
2. checking what the user may or may not do
3. auditing actions
4. deciding and controlling how addresses are to be managed
5. being alert to abnormal behaviour
6. ensuring that sensitive data is encrypted during transmission
7. configuring the system so it offers a minimum of services
8. ensuring that data is encrypted the whole way, end-to-end, and not only over the wireless interface.

8 A public authority in Canada provides advice to SMEs

In Canada, advice is provided on the website 'Canada's business and consumer site' <http://strategis.ic.gc.ca/engdoc/main.html>, which is part of Industry Canada. This authority corresponds to the Swedish Ministry of Industry, Employment and Communications. The mission of Strategis is to utilise the power of the Internet and to work together with Canadians in order to establish a knowledge-based and growing economy. Its advice is directed at SMEs, see <http://www.strategis.ic.gc.ca/epic/site/dir-ect.nsf/en/uw00354e.html>.

This advice includes the use of security measures, such as:

1. using encryption, such as WPA, Internet Protocol Security (IPSec) or a VPN solution
2. being alert to employees connecting their own equipment for wireless local area networks
3. monitoring the wireless local area network in order to identify false access points, trace intruders and prevent threats as well as introducing a security policy for WLAN use.