Commission for
Communications Regulation

Briefing Note Series

Security Implications for New and Emerging Telecommunications Technologies

Document No:	**04/29**
Date:	**12th March 2004**

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
Abbey Court Irish Life Centre Lower Abbey Street Dublin 1 Ireland
Telephone +353 1 804 9600 *Fax* +353 1 804 9680 *Email* info@comreg.ie *Web* www.comreg.ie

Contents

1 Comments on this Briefing Note

We welcome any comments or views on this Briefing Note and these should be sent to:

Jonathan Evans
Market Development
Commission for Communications Regulation
Irish Life Centre
Abbey Street
Dublin 1
Ireland

Tel: +353 1 8049709 Fax: +353 1 8049680
E-mail: jonathan.evans@comreg.ie

to arrive on or before Friday 23rd April, 2004.

Comments will be reviewed by ComReg when carrying any out further work on issues covered in this Briefing Note. In submitting comments, respondents are requested to reference the relevant section of this document. Responses will be available for inspection by the public on request. Where elements of any response are deemed confidential, these should be clearly identified and placed in a separate annex to the main document.

Disclaimer
This document does not constitute legal, commercial or technical advice. The Commission for Communication Regulation is not bound by it. This document is issued without prejudice to the legal position of the Commission for Communications Regulation or its rights and duties under relevant legislation and does not form part of any formal tender process.

This document is for information purposes only and is not intended to give any indication of ComReg policies, current or future, relating to any of the issues raised, or to any alternative technologies not included here.

2 Executive Summary

This Briefing Note is the fifth to be published following the first meeting of the ComReg 'Forward-looking Programme Steering Panel'[1] in May 2003. At this meeting the Panel identified some key Briefing Note topics. One of these topics was the security and privacy implications of new and emerging telecommunications technologies. The purpose of this document is to help raise awareness of the types of security threats consumers are likely to experience as they adopt new technologies and the measures that they can take to protect against these threats. For users to gain the maximum benefit from these technologies they need to be able to trust them. Hence consumers need to understand the threats that can arise and ways in which they can protect themselves. This note aims to explain some of these issues for end users, and to highlight their importance to operators and systems developers. Briefing Notes are primarily intended for non-technical readers with some background knowledge of telecommunications.

Widespread availability and take-up of always-on broadband access will bring users many benefits that will enable them to participate in the Information Society. Enhanced security systems can be deployed by network service providers and end users to deal with the potential increase in malicious encounters that they are likely to experience as broadband adoption grows. Other new technologies such as sophisticated mobile phones are capable of running software applications that are downloaded wirelessly over the Internet (e.g. smart phones). These could leave users vulnerable to many of the security and reliability problems that users and IT administrators have had to deal with on PCs and the fixed Internet (e.g. viruses and hackers). Generally speaking, with new technological developments and an increased volume of security threats, there is a greater need for more security awareness and understanding among everyday users. New initiatives from telecommunications service providers and more secure, user friendly products from software developers are likely to help improve security for end users as they adopt new technologies. However, there are many measures that end users themselves can take to ensure they retain their privacy and security. Among these measures, users should ensure security features and settings are activated and that anti-virus and other software is kept up to date, when connecting to the Internet with computers or advanced mobile phones. Users should also generally avoid pirated software, activating unknown applications and responding to suspicious messages.

Although the security and privacy threats are increasing, so are technology developments aimed at countering them. If consumers take sensible security precautions and deploy appropriate new security measures there is no need for it to deter adoption of new telecommunications technologies. The benefits of new technologies can by far outweigh the potential risk posed by computer vulnerabilities.

[1] The Steering Panel consists of a small group of senior external experts, serving in their individual capacity, from Ireland and overseas, who have agreed to advise ComReg on its Forward-looking Programme. See Annex 1 for a list of the panel members. The group highlights and discusses future technology developments and related issues that could impact the development of the Irish telecommunications market. The Programme typically looks two to six years ahead. Its purpose is to help ComReg anticipate technological trends and developments in order that these can be taken into account in shaping ComReg's strategy and its future work programme.

This document outlines the types of security risks associated with some key technologies that are either emerging or will soon be ready for widespread adoption. The note covers the main categories of security threat faced by developing technologies, but it is not intended to be a complete listing[2]. It goes on to explain the types of security technologies and practices that can be applied by everyday users to help protect themselves from the majority of attacks. Measures to improve software and systems are also outlined.

[2] Note: Examples of specific security problems and solutions are listed throughout this document. These are merely illustrative examples and are not intended to focus on any individual companies or products in particular.

3 Introduction

3.1 Trusting computers with our information

Communications and computing technologies are continuing to converge and we are continuing to integrate them into our lives. For example our personal details such as financial and medical records can all be stored and transmitted electronically. We can access much of this information through the Internet via home computers, Internet cafés, and our mobile phones. This increasing reliance on technology and on new ways to remotely access personal information can bring about new risks. In general, the potential security risks increase as more information is stored on computers, and as those computers are connected to an increasing number of other computers (e.g. the Internet). Therefore there is a trade-off between the benefits of networked communications and greater participation in an information society on one hand, and increased security vulnerability on the other hand. It is natural for people to be distrustful of new technologies particularly where personal details are concerned. In order to trust computer systems users should expect certain secure characteristics as they use them to communicate. Characteristics such as integrity, reliability, availability, confidentiality (and business integrity), privacy and resilience are all important to end users[3]. Having learned to exercise care and vigilance when operating computers connected to the fixed Internet, users will soon have to adopt similar practices when using mobile and portable devices as more advanced systems give them greater access to the Internet, (section 5 outlines ways for users to protect themselves against common threats). Increasingly we can also expect to see computing devices integrated into everyday objects. This is known as pervasive or ubiquitous computing. Developments such as these require users to be aware of security whenever they interact with information technology.

3.2 Remaining secure

High profile cases of computer security breaches such as prolific viruses and Internet scams often draw media attention. This can cause wariness among potential adopters of new telecommunications and computing technologies, which can in turn deter them from adopting such services. The numbers of passwords and complex procedures that we are expected to manage to carry out everyday tasks can seem frustrating at times. Furthermore, an array of different types of security threat such as viruses and hackers can leave users confused. However, by implementing some relatively simple security precautions, such as personal firewalls, and keeping anti-virus and other software up to date, users can avoid the majority of security threats. This is analogous to a home burglar alarm system where, although penetrable to a skilled and motivated thief, the threat from unskilled opportunistic thieves is greatly reduced. In many cases there is a trade off between security and ease of use for end users.

3.3 The security systems 'arms race'

Security systems developers have been in a continuous race against those who attempt to abuse ICT[4] systems (e.g. computer hackers[5]), and this is likely to remain so

[3] See Microsoft's Trustworthy Computing Initiative – http://www.microsoft.com/mscorp/twc/default.mspx

[4] Information and Communications Technology

regardless of technology developments that may occur[6]. As soon as a new system or software product is released, computer hackers begin seeking out flaws to exploit. Software developers then typically respond with an updated piece of software that users can add to their systems to protect against such attacks (see section 5.2). Significant new developments in the way we use communications technology such as widespread broadband adoption and the development of advanced mobile handsets are uncovering new security threats that need to be addressed.

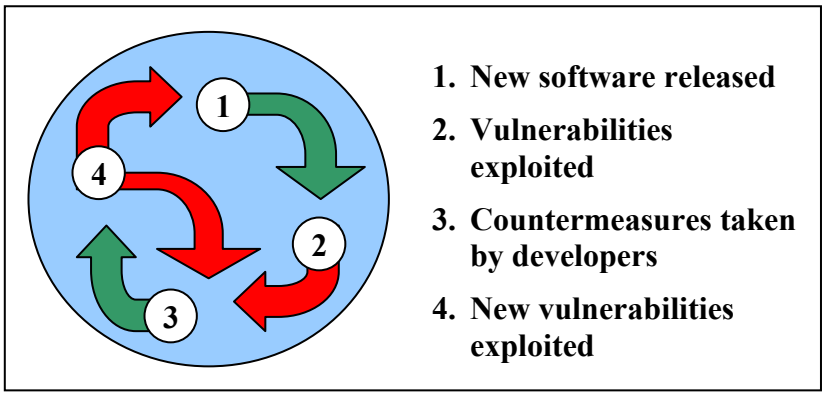

Figure 1. Typical security developer and hacker relationship

[5] In this document the term computer hacker is used to describe malicious users of computer and communications systems (e.g. virus creators, fraudulent users, denial of service attackers, unauthorised users of computer systems).

[6] With the possible exception of quantum computing which is an advanced research area that could potentially enable instantaneous processing of complex computations.

4 Technology and Vulnerabilities

This section outlines some of the important technologies that are now emerging that will have implications for user security. Common security threats are also outlined here. The next section (Section 5) highlights some technologies and methods to deal with these security threats.

4.1 Always-on Broadband

Computers are potentially vulnerable to security threats any time that they are connected to the Internet. With always-on broadband services the time that users are potentially exposed to hackers is greatly increased, compared to dial-up Internet users who are typically only connected to the Internet for relatively short periods of time. Although the general level of vulnerability is the same for dial-up and always-on broadband users, the risk to always-on users is increased because their computers are connected to the Internet for longer periods of time. Always-on connections also are likely to be left unused for a large portion of time[7]. This problem exists for always-on access regardless of the technology being used (e.g. DSL, Cable, Fixed wireless, mobile, satellite). Another problem with broadband connections compared with slower Internet connections (e.g. dial-up modems) is that hackers can use the high speed connections to attempt more methods of attack within a given period[8]. High speed connections enable hackers to get in and out of your system in a shorter time, reducing the chance of detecting them. Telecommunications service providers typically assign always-on broadband users with fixed Internet (IP) addresses, for a reasonable length of time, as opposed to dynamic addresses that change each time a user connects on a dial-up system. A fixed IP address makes it easier for a hacker to return to a weak system to re-exploit it.

High capacity connections belonging to broadband users are attractive to hackers seeking to carry out more damaging attacks on others (e.g. distributed denial of service attacks). A study from the NIST in the US showed that on average more than three potentially serious intrusion attempts were made daily on a single broadband connection[9].

In addition to attacks through the Internet, in some cases hackers can target the transmission medium directly (i.e. by listening in on wires, cables, radio frequencies). In a cable modem system multiple users (typically over 100) share a single high capacity co-axial cable. To prevent users eavesdropping on other users on the same cable access is generally restricted in each cable modem allowing each user to only view their own traffic. Hackers can target the cable modem itself allowing them to view other users' traffic on the shared cable, provided that encryption[10] has not been implemented. Encryption also needs to be implemented on radio systems to protect users from eavesdroppers.

---

[7] In some cases where users do not need always-on connectivity at all times (e.g. during the night) it would be advisable for them to turn off their always-on connections to reduce the risk from hackers. Such users would still avail of the full benefit of always-on connection during the day while they are more likely to be using their computers.

[8] See "Got Broadband? You're under attack", http://www.extremetech.com

[9] This study was carried out using an always-on broadband connection left continuously active for 10 full days. 'Security for Telecommuting and Broadband Communications' National Institute of Standards and Technology, US Dept. of Commerce, August 2002

[10] See section 5.9 for an explanation of encryption.

Without adequate security protection one vulnerable group of broadband users are tele-workers. Tele-workers often need to access and share confidential or commercially sensitive information with colleagues and customers. An organisation which deploys tele-workers must ensure that the necessary security features (e.g. a secure VPN – see Section 5.4) are in place and that security policies are followed by the tele-worker[11] to maintain secure information systems. It is worth noting that the distributed architecture of the Internet can make it difficult to provide widespread security. End to end solutions are needed for the Internet, which can be difficult to implement.

4.2 Mobile Handsets and Systems

Mobile handsets have traditionally only had simple operating systems designed to cope with telephony services. However, mobile phones and other devices are quickly developing from single purpose communications devices to multi-purpose computing and communications devices, and users are generally not aware of the associated potential security vulnerabilities. More sophisticated mobile handsets such as smartphones and PDAs are now available that download software wirelessly over the Internet[12]. The types of handsets that are being developed for 3G services will have this level of functionality. The extra functionality that is brought about by being able to install new software applications creates a potential risk of exposure to viruses and computer hackers. Furthermore as wireless functionality is integrated into more and more computing devices such as laptop computers via wireless LAN equipment these devices are also becoming potentially vulnerable to security risks. Devices also become more vulnerable as they begin to have their own IP addresses.

The use of multiple different types of communications methods (e.g. via cable, wireless LAN, infrared, wireless mobile, Bluetooth[13]) in a single device such as a laptop computer is also becoming more common. Such devices present a complex environment for security management. Developments in mobile computer processing, storage and display technologies are leading to more powerful mobile devices. As users continue to operate a number of different devices (e.g. desktop PCs, handheld computers, smart phones) they need a consistent level of security across all platforms.

The small size of handheld devices make them easier to misplace and more likely to be stolen[14]. Limited computing power on handheld devices, compared to fixed desktop devices, may make it less practical to operate the same level of security or strong encryption software. As with fixed broadband connections, 3G devices which provide always-on connectivity are also more exposed to security threats than their connection orientated (i.e. 2G) predecessors. However, personal firewalls are

[11] e.g. users may only be permitted to access the organisation's network via the equipment they have been allocated and not by other un-authorised personal devices such as wireless LAN devices for example – see Section 4.2.1.

[12] "Smartphones outsold PDAs 2:1 last quarter", The Register, 26 January 2004

[13] Potential security threats to Bluetooth systems were recently highlighted - http://www.atstake.com/events_news/press_releases/template.html?europe/121603 , http://news.zdnet.co.uk/communications/wireless/0,39020348,39145881,00.htm

[14] Such devices are also easier for to conceal for thieves.

available for some handheld devices (e.g. Bluefire[15]). Active content and moveable code (see Section 4.4) is also a threat for advanced mobile handsets.

4.2.1 Wireless LAN vulnerabilities

The security issues associated with implementing a wireless LAN are not always well understood by IT managers, which in the past partly led to a reluctance to install such systems despite the benefits that can be achieved[16]. However, it is true that without security provisions in place (see Section 5.3) Wireless LANs provide a very easy way for hackers to listen in on or access a private network. Tools are readily available on the Internet for users to breach poorly configured and outdated wireless LAN security (i.e. war-driving)[17]. Employees who introduce their own readily available wireless equipment to corporate networks without informing IT staff can introduce security weak points. In this case security on the entire corporate network can be unknowingly comprised by the user, despite the existence of corporate security solutions[18]. It is typical for wireless LAN equipment to be shipped with security features disabled by default. Without proper configuration, this can potentially open up an otherwise secure network to attack. Many home users are choosing WLAN equipment to set up wireless networks within their homes. Such networks can be for sharing common computer peripherals such as printers and scanners, and for sharing a broadband Internet connection (e.g. DSL[19]) without the need to install network cables throughout the home. Unless securely configured, these networks can also present a security threat to home users.

4.2.2 Software Defined Radio

Future mobile devices and systems which are even more programmable such as software defined radios (SDR)[20] could potentially be vulnerable to viruses and hackers. It is conceivable that SDRs could be reconfigured by hackers to carry out illegal transmissions causing interference to legitimate radio services. This type of attack could be carried out as a distributed denial of service attack. SDRs are likely to need firewalls and secure authentication systems to protect themselves from such attacks if they emerge.

4.3 Voice over IP (VoIP)

VoIP systems create new opportunities for hackers to attack telephone services (known as 'phreaking'). It is therefore possible that as VoIP services become more commonplace, traditional telephone users could be subjected to some new threats[21].

---

[15] http://www.bluefiresecurity.com/mobile_firewall_plus.php

[16] One high profile example of Wi-Fi being dismissed due to security concerns was by the International Olympic Committee in 2002. They decided to hold off on deploying Wi-Fi as part of the IT infrastructure at Olympic games until 2008 when stronger security should be established. See 'Security fears mean Wi-Fi won't star at the Olympics', ZDNet UK, July 2003.

[17] On a busy network (e.g. a corporate WLAN) hackers can collect enough information in a couple of hours to crack WEP (see Section 5.3) security systems. The term 'war-driving' comes from the earlier term 'war-dialling' which was a method of hacking telephone systems.

[18] This is equivalent to someone leaving a single window open in a building where the owners have taken the trouble to lock all of the doors.

[19] e.g. see recent eircom offer: http://tinyurl.com/2bfy5

[20] See ComReg briefing note – http://www.comreg.ie/_fileupload/publications/odtr0159.pdf

[21] e.g. http://www.security-corporation.com/articles-20030824-001.html

The two main standards for VoIP are Session Initiation Protocol (SIP) and the ITU standard H.323 (see ComReg Briefing Note on VoIP[22]). Both standards offer encryption. Additional security such as IPSec is typically used when deploying VoIP on virtual private networks (see Section 5.4).

There are concerns from law enforcement agencies in the US that advanced voice networks are too secure to allow lawful wire-tapping. It is generally difficult to decode encrypted voice in real-time. VoIP security is generally dependent on the overall security of the data network that voice is running over.

4.4 Active Content

Active content is data that can initiate or carry out actions on a computer without the intervention of a user[23]. This type of code is now common-place and is used for applications such as animating web-pages and calculating formulas within spreadsheets for example[24]. Active content poses more of a threat to security than older systems where data was clearly separated from instructions, because it provides a way for malicious instructions to be hidden. Java, Active X, scripting languages (e.g. JavaScript), and plug-ins (e.g. RealPlayer) are examples of active content. Mark-up languages can also be used to contain instructions (e.g. XML). Authentication processes and usage policies are commonly used to help users securely use active content.

4.5 Peer to peer applications

Users of peer to peer applications[25] will need to be extra vigilant against security threats from viruses and hackers. If not carefully managed, users can unwittingly give access to personal or sensitive files on their computers while trying to share certain content. By giving other users access to share files on their computers they are potentially exposing their systems. Other issues such as piracy of copyright material and storing of illegal material can be an issue for employers who find that their employees are storing such information on their networks. The very nature of decentralised peer to peer applications is at odds with most telecommunications security techniques that rely on centralised servers. Most high profile security threats on peer to peer networks have been worms (see Section 4.7.2). The recent MyDoom worm which in some cases makes use of directories shared by P2P programme Kazaa is reported to have been the fastest spreading virus so far[26]. Tighter security measures for peer to peer systems are being developed by companies such as Microsoft, Sun Microsystems and IBM, but this will not help the current peer to peer applications already implemented.

---

[22] http://www.comreg.ie/_fileupload/publications/ComReg0321.pdf

[23] See "Guidelines on Active Content and Mobile Code", National Institute of Standards and Technology (NIST) Special Publication 800-28, October 2001.

[24] PostScript for printing documents is an early example of active content.

[25] See ComReg briefing note -http://www.comreg.ie/_fileupload/publications/ComReg03110.pdf

[26] At its peak one in every twelve email messages was estimated by MessageLabs to contain the MyDoom virus.
http://www.messagelabs.com/news/virusnews/detail/default.asp?contentItemId=734&region=

4.6 Software Vulnerabilities and Complexity

Hackers regularly attempt to seek out and exploit flaws (i.e. bugs) in software as soon as it is released by creating viruses or directly accessing systems that use this software. Many attacks are aimed at known weak spots in software programs, and often target flaws in operating system or Internet browser software. After-market discovery of such flaws causes software developers to continuously issue additional pieces of software (known as 'patches') to rectify these problems. For effective security users need to keep their systems updated with all of these patches as they emerge. In other cases hackers can exploit the actual code that makes up an application. This is known as 'source code' and is generally closely guarded by commercial software companies, but can on occasion fall into the hands of hackers[27].

Configuring security software and security features within software applications can be too complex a task for mass market users. The result is that in many cases available security features are not configured correctly (e.g. the default user settings are left in place) or even activated. This is a significant problem that needs to be addressed by the software industry if users are to adopt the security measures already available to them. Future security features will need to be simpler to use to make them more accessible to non-technical users. There is also a need for greater integration between different security applications from different vendors to help simplify the increasingly complex task of managing security systems and passwords for users. End users would benefit from the development of more integrated security systems that include their various different accounts, devices and access methods.

4.7 Hackers and Viruses

4.7.1 Types of attack

Generally speaking attacks on computer systems can be random or targeted. Most attacks that typical telecommunications users are likely to encounter are of the random variety (e.g. viruses, port-scanning[28] etc.). Attacks that are targeted at specific users or systems are generally carried out by more experienced hackers with more focused objectives (e.g. to steal commercially sensitive information or financial details). Targeted attacks can include denial of service attacks. Attacks can also be described as passive or active. Passive attacks involve eavesdropping on victims to collect information such as passwords or credit card details. Active attacks can involve attaching malicious data onto a victim's system (e.g. defacing a website)[29]. Some common types of computer attacks are described below.

Denial of Service – This is where the hacker utilises systems belonging to innocent users to assist them in overloading a victim's system with data (e.g. a corporate website). Distributed denial of service (DDOS) attacks make use of multiple users' computers to initiate a co-ordinated attack on a victims system. To initiate such an

[27] Many software applications are developed using 'open source' software, where the source code is readily available. Security for these systems needs to be designed with this in mind.

[28] While port scanning is not strictly speaking an attack, it is a method used by hackers to identify potential weak points on a computer system that they could exploit. Port scanning is also used by system administrators to identify vulnerabilities on their networks.

[29] It is also worth noting that in some cases curious, but unskilled, users can unknowingly cause disruption to computer systems.

attack individual computers (known as 'zombies') are infected with a virus that spreads and often lies dormant until a specific coordinated time.

Identity theft – This is when someone uses your personal details such as your name or credit card number, without your permission, to carry out some crime or fraudulent act[30]. Identity theft can result in bad credit ratings and other financial problems, that often continue to resurface (i.e. as their personal details are sold on) for years after the initial theft.

Low-tech Attacks - There are many programs, procedures and code available on the Internet that can allow relatively unskilled hackers to attack computer systems. These types of attackers are often known as 'script kiddies' and are generally more of nuisance than a serious security threat. In some cases these attacks can be launched through websites set up by hackers to facilitate less skilled hackers. The accessibility of such hacking tools, known as 'point and click' tools, could potentially lead to an increased number of low-tech attacks. There is a concern that a multitude of low tech attacks could act as a smoke screen for a skilled hacker to hide behind.

Back doors – These are programs that once installed on a victim's system allow remote users (i.e. hackers) to access and control parts of the victim's system. Back door programs can be spread through emails.

Phishing – Authentic looking messages that appear to be from legitimate sources (e.g. an on-line bank) but with links directing users unknowingly to counterfeit websites that trick them into divulging their account details and passwords[31]. This type of fraud is known as 'phishing' or 'carding'[32], and Microsoft recently updated a flaw in their Internet Explorer browser that was being used for this[33]. Users can generally avoid these scams by being vigilant and suspicious of any emails that unusually request you to update personal details, and by not clicking on links (hyperlinks) in emails themselves. In other cases bogus emails can contain attachments claiming to be anti-virus software updates, when they are in fact viruses themselves (e.g. swen worm[34]).

Resource Stealing – In some cases hackers target broadband users to make use of their, often under utilised, high speed communications and computer resources for illegal purposes. For example, a hacker could access a user's system to set up an Internet relay chat (IRC) server without the user's knowledge. In other cases groups of hackers can use a victim's computer and Internet connection as an illegal repository for data such as pirated music, video and software.

Spam – Spam (sporadic mail) is an unwanted nuisance that can disrupt how we use the Internet. While not strictly speaking a security threat on its own spam can be

[30] http://www.consumer.gov/idtheft/

[31] http://www.pcworld.com/news/article/0,aid,109718,00.asp

[32] http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

[33] http://news.bbc.co.uk/1/hi/technology/3454289.stm

[34] http://www.internetweek.com/security02/showArticle.jhtml?articleID=15000773

used as a vehicle to distribute viruses and worms. Spam can also be used to carry out fraud through 'phishing' attacks (see above). To help keep spam under control, users can maintain spam filtering programs, some of which are freely available (e.g. Spamassassin[35]). This is another additional administrative task that users must tend to in order to maintain their computers and communications systems in proper working order. Initially a problem on fixed networks, this is now becoming a significant problem for mobile systems too (e.g. SMS spam). Bluejacking is the term given to sending anonymous messages between Bluetooth devices which could be used as a type of short range (approximately 10 metres) spamming[36]. (see Section 6 for initiatives on combating spam).

4.7.2 Viruses

The term virus or malware (malicious software) is commonly used to collectively describe several different security threats including viruses, worms, trojan horses and malicious mobile code. These are all sections of computer code written and distributed with the intent to disrupt computer and communications systems. Some of these are used to destroy data indiscriminately on any computers which become infected, while others are designed to replicate themselves and launch co-ordinated attacks on specified computer systems (see Denial of service above). Other viruses are relatively harmless and are often written to highlight security flaws in systems. Viruses are typically spread though email attachments, Internet browsers, removable media (e.g. floppy discs), and downloadable software (e.g. some shareware and pirated software (also known as warez)). In the future it is likely that virus creators will find even more sophisticated ways of propagating viruses possibly through techniques such as steganography or digital watermarking which are used to hide data within images or other files. The main categories of virus are briefly described below:

Virus – computer code that, when activated, uses the resources of a computer programme or document that it is attached to, to replicate itself, and carry out some predefined and often malicious actions.

Worm – a computer programme that can replicate itself onto other computer systems, without user intervention, to carry out damaging actions.

Trojan Horse – this is a computer programme that carries out malicious actions while pretending to do something useful for the user.

Malicious Mobile Code – Mobile code such as Java and ActiveX (see Section 4.4) is used by websites to add functionality. This is code that can be moved between different systems and is still able to carry out the same instructions. Malicious mobile code takes advantage of security vulnerabilities in mobile code to infect users.

4.7.3 Spyware

This is software that once installed on your computer can report details of what Internet sites you have visited back to a website somewhere without your knowledge. This type of technology could potentially be used to collect sensitive

[35] http://news.spamassassin.org/

[36] http://www.bluejackq.com

personal information about users. Internet 'cookies' which store information about what websites a user has visited on a users computer can be considered as a type of spyware. However, cookies provide important functionality for Internet websites and are used for legitimate marketing purposes.

Attack Type	Origination/ Targeted Weakness	Effect/Damage	Protection
Identity Theft	hacked systems, user complacency	loss of money, credit rating problems,	manage passwords, vigilance
Virus Worms Trojan Horses	email attachments, Internet downloads, removable media (discs), operating system vulnerabilities	Loss of data, computer system corruption, hardware damage[37], embarrassment	updated anti-virus software, and operating systems
Phishing	user complacency,	identity theft	vigilance
Spam	email, text messages	nuisance, can spread viruses	spam filtering software
Denial of Service	email, Internet	loss of communications	firewalls with traffic monitoring
Spyware	Internet, downloaded software	loss of privacy	spyware removal software

Table 1. Common security threats.

[37] e.g. Win95/CIH virus damaged flash memory chips, requiring a replacement of the motherboard in some computers.

5 Security Technology and Best Practices

5.1 User Responsibility

The first, and most effective, defence against hackers and other security threats is for users to take responsibility for their own security and learn to exercise vigilance and discipline when it comes to networked communications. Simple steps such as ensuring that built in security features are activated (e.g. on Internet browsers or operating systems) and anti-virus and other software is kept up to date can help users to protect themselves against the majority of opportunistic and random attacks. Users should delete any suspicious looking emails from unknown senders, particularly if there are files attached, and they should under no circumstances open unknown applications. To minimise the damage that viruses can cause, users should make regular backups of their important data. Currently these precautions apply mainly to fixed Internet communications such as broadband DSL services, however similar care will be needed with mobile devices and software as they become more sophisticated. Users should also be careful about who can physically access their systems (i.e. PCs, Laptops, mobile phones, etc. left unattended). If users are sharing equipment (e.g. in a small office/home office environment) they need to be aware of what software is being installed by other users to ensure that it does not compromise their overall security. Setting out a security policies helps to clarify best practices for end users, reducing the possibility of them accidentally causing security breaches.

5.2 Anti-Virus and Security Software

If kept up to date, anti-virus software is an effective way for users to protect themselves against damage from computer viruses. These are software programs that can scan all incoming files and emails for the presence of known viruses. Anti-virus software producers (e.g. Symantec, McAfee) typically offer regular up-grades which users can download over the Internet, to ensure protection against the latest viruses as they emerge[38]. This can typically be configured to operate automatically via users' internet connections. Some anti-virus software is available for free (e.g. AVG Anti-Virus System[39]). Microsoft[40] and other targets of software viruses regularly offer large rewards for information leading to the arrest and conviction of those responsible for creating these viruses.

5.2.1 Firewalls

Users can also install personal firewall software (or dedicated hardware firewalls such as those that might be implemented in a corporate network) on their computers which can be configured to only allow communication with applications that have been authorised and authenticated. This can greatly reduce a user's vulnerability to hackers. A useful feature of many firewall systems is being able to log and review all activity that has passed through the firewall. This can allow users to identify unauthorised applications so that they can take action to stop further attacks. Greater simplification in the configuration and use of personal firewalls could assist end users in making their systems more secure.

[38] These upgrades come in the form of larger 'virus definitions' files, which contain protection against all the known viruses at that time.

[39] http://www.grisoft.com

[40] e.g. The Microsoft Anti-Virus Reward Scheme: http://www.microsoft.com/security/antivirus/

5.2.2 More sophisticated anti-virus software

New techniques are developing that can help to predict the nature of future attacks from computer hackers, and such techniques may eventually be applicable to viruses and other security threats[41].

In many cases anti-virus filters attached to email servers can add to the problem of email spread viruses by returning rejected message to the address that they appear to come from (which has often been faked). In some cases copies of the virus are sent on along with the notification message thus increasing the spread of the original virus. A standardised approach from the anti-virus industry to identifying and naming new viruses would help with the management of emailed virus reports.

Viruses that use vulnerabilities exposed by previous viruses have emerged whose purpose is to patch up security flaws. These are known as 'white hat' viruses. For example a recent variant of the Nachi worm cleanses computers infected with the MyDoom virus and loads Microsoft security patches from the Internet[42]. The use of such techniques to fight computer viruses is generally considered unsafe and can cause systems to fail due to excessive traffic.

5.2.3 Online Security Assessments

Users can check for vulnerabilities on their computer system by using an online security assessment programme. These programs scan your computer and Internet connections for potential security weak spots and notify the user[43]. Users must be sure of the authenticity of such services over the Internet, before divulging sensitive details about their computer systems.

5.2.4 Spyware Removers

Software is also available (freely in some cases – e.g. Ad-aware from Lavasoft), that can detect spyware on a system and remove it. In some cases commercial software will not function if their associated legitimate spyware is removed. In such cases the user agrees to the installation of this spyware when they agree to the licence conditions.

5.2.5 Tackling Spam

Developments in the area of spam are emerging that could help users avoid a large proportion of the spam that they receive. Yahoo! is implementing a system called Domain Key that adds a digital authentication to emails for companies and organisations[44]. Research into other techniques is being carried out by the Internet

[41] "Mutating software could predict hacker attacks", New Scientist, 25 January, 2004

[42] http://www.theregister.co.uk/content/56/35524.html

[43] See http://www.dslreports.com/tools/

[44] PGP (see Section 5.9) can also be used to authenticate email signatures to help reduce spam.

Research Task Force of the IETF[45] and a sender policy framework (SPF) that could help reduce spam through the use of false addresses is being developed[46].

New initiatives to tackle the problem of spam involve incurring a charge on senders of emails or requiring that a computer performs a time consuming computation before sending an email which would mean that spammers would need huge computing resources to send multiple messages. Both of these ideas have been proposed by the Microsoft project "Penny Black" in its efforts to eliminate spam[47].

Internet Service Providers and other telecommunications operators can take a more active role in preventing abusive use of the Internet to carry our denial of service attacks by closely monitoring their traffic, enabling them to shut down any suspicious traffic patterns (e.g. TeliaSoneria). Both O2 and Vodafone have taken measures in Ireland to tackle mobile spam[48].

5.3 Wireless LANs (Wi-Fi)

Wireless LANs have often been perceived as being insecure through a combination of poor configuration and weak security standards (i.e. Wired Equivalent Privacy). Until recently enterprises were left to implement their own third-party security solutions such as virtual private networks to secure their WLAN networks. The IEEE[49] and the Wi-Fi Alliance have now addressed the problem of poor WLAN security with the Wi-Fi Protected Access standard. It is now up to users to ensure that they install and configure the security standards available to them to protect themselves from hackers.

Wired Equivalent Privacy (WEP) – This security standard is incorporated in the IEEE 802.11b standard and has known weaknesses.

Wi-Fi Protected Access (WPA) – This security standard is a subset of, and will be compatible with, the IEEE 802.11i security standard (also known as WPA2) currently being drafted. WPA addresses all of the known weaknesses of WEP (e.g. user authentication and encryption keys) and is released as an interim standard while 802.11i is being developed[50]. The Wi-Fi Alliance has announced that it will produce an updated version of WPA in 2004. All future Wi-Fi products must have WPA to achieve Wi-Fi Alliance certification. Over 175 Wi-Fi products have been certified as being compatible with the WPA standard[51]. WPA is designed to work on existing Wi-Fi devices (802.11a, b, g) through a software download. WPA eliminates the need for added on wireless security products to protect Wi-Fi networks.

---

[45] See http://asrg.sp.am/ The Internet Engineering Task Force (IETF) are an international community of network designers, operators, vendors and researchers (http://www.ietf.org)

[46] http://www.ietf.org/internet-drafts/draft-mengwong-spf-00.txt

[47] "Microsoft project aims to make spammers pay for spam", Feb 2004, Total Telecom.

[48] http://www.enn.ie/frontpage/news-9388007.html

[49] Institute of Electrical and Electronic Engineers

[50] WPA uses Temporal Key Integrity Protocol (TKIP) with a dynamic 128 bit key for encryption and 802.1X with Extensible Authentication Protocol (EAP) for authentication. Users and workstations require a software upgrade to employ WPA. Enterprises require an authentication server (e.g. RADIUS – Remote Authentication Dial-In User Service). Home or SOHO users can manually configure their networks with a 'pre-shared key' (PSK) password.

[51] See http://www.wi-fi.org/certified_products for a database of certified products.

IEEE 802.11i (WAP2) – The IEEE 802.11i standard is expected to be completed in 2004. In addition to all of the features in WPA, 802.11i includes another stronger form of encryption known as Advanced Encryption Standard. Although IEEE 802.11i will in many cases require new hardware (e.g. Wi-Fi cards and access points) it can be operated alongside WPA during migration.

5.4 Virtual Private Networks

Virtual private networks (VPNs) can be set up to provide increased security where users may need to remotely connect to a corporate network for example. Security measures for VPNs include IPSec[52] and SSL (see Section 5.9). This type of network can be important for organisations wishing to deploy tele-working. Setting up and administering a secure VPN is typically carried out by skilled IT professionals. Authentication for remote users is often carried out using a Remote Access Dial-In User Server (RADIUS).

5.5 IPv6

Internet protocol version 6 (IPv6) can potentially allow for increased security by enabling greater authentication and control over IP communications[53]. IPv6 is an updated version of the protocol used by Internet technology.

5.6 Voice over IP (VoIP)

Some VoIP service providers encrypt their traffic to offer users privacy (e.g. Skype). Traditional firewall products were not designed to handle real-time IP traffic such as voice. Newer firewalls (known as Real-Time Firewalls (RTF)) are now available that can accommodate VoIP. It is worth noting that on corporate networks data can often be more sensitive than voice communications, and the network is likely to be secured to this higher level.

5.7 Robust Software and Systems

The importance of robust and reliable software is often only too apparent as most hackers and viruses tend to attack vulnerabilities caused by flaws in software. Many software programs are released without taking sufficient care to ensure that they do not contain vulnerabilities that could be exposed by hackers. Higher standards across the software industry could lead to more secure applications and systems while also reducing inconvenience due to software bugs. Microsoft's Trustworthy Computing Initiative[54] is attempting to address this issue. The IETF has numerous work streams dedicated to security on IP networks[55].

[52] The IPSec protocol is an extension of the IP protocol that can be added to provide security on IP networks. IPSec allows corporate users to avail of secure VoIP services over VPNs.

[53] See ComReg Briefing Note on IPv6 – http://www.comreg.ie/_fileupload/publications/odtr0263.pdf

[54] http://www.microsoft.com/mscorp/twc/default.mspx

[55] http://sec.ietf.org/

5.8 Digital Signatures

Digital signatures are used to authenticate data and users, ensuring that when data is received it can be guaranteed that it has been sent from a particular user and that it has maintained its integrity. Digital signatures are also used in case someone disputes that they have sent something that you received from them (i.e. non-repudiation).

Public Key Infrastructure (PKI) describes the processes, policies and standards that are involved in authentication and encryption of data. See section 5.9 for more details on encryption.

Extensible mark-up language (XML) is being standardised for use in digital signature[56] and encryption ('XML Signature' and 'XML encryption'). XML signatures can be assigned to specific parts of an XML document. This facilitates multiple parties to modify documents while allowing individuals to take responsibility and ownership of certain parts only.

5.9 Encryption

Encryption can be used to keep a user's information private either during transmission over insecure networks such as the Internet or while it is stored on computer systems[57]. Encryption is a mathematical process used to make information unintelligible to unauthorised users. Authorised users are able to decrypt the encrypted message to reveal the original information. Information is encrypted and decrypted by entering it along with a string of data, similar to a password, known as a 'key' into a mathematical formula (which is typically publicly known and standardised). There are two main types of encryption: private (secret) key and public key encryption. Private key encryption uses the same key to encrypt and decrypt information. In this case users must take care to keep the key secret because anyone with a key would be able to interpret the original information. Public key encryption uses two keys: a public key and a private key. The public key is used to encrypt the information and can be made known to others because only the private key can be used to decrypt the information. A user wishing to receive encrypted information sends their public key to the sender of the information. The sender then uses the receiver's public key to encrypt the information and transmits it. This message can now only be decrypted using the private key which is only held by the receiver. This is equivalent to sending someone an open padlock (i.e. the public key) for which you have the only key (i.e. the private key), the recipient of the padlock puts their message into a box (i.e. the encryption algorithm) and locks it with your padlock before sending it to you. Then only you can unlock the box because you held onto your key and did not have to send anyone a copy of it. Public key encryption was first developed in the mid 70's and is now used for most e-commerce and secure transactions over the Internet.

Secure Multipurpose Internet Mail Extensions (S/MIME)[58] and Secure Socket Layer (SSL[59]) are examples of commonly used security services that employ encryption[60].

---

[56] XML Signature is being standardised in a joint effort by the IETF and the World Wide Web Consortium (W3C). See http://www.w3.org/signature/

[57] It is worth noting that most hackers would generally be more interested in targeting databases on an organisation's network that contain credit card details for example than trying to intercept individual packets of information while in transit.

[58] http://www.imc.org/smime-pgpmime.html

Encryption can have performance implications for systems as it involves processing all data through mathematical algorithms. Communications systems need to be designed with encryption in mind. 'Key' distribution and management is a challenging issue for encryption systems. Research is currently under way on developing future systems that will implement quantum key distribution techniques making it more difficult to intercept a key without being detected[61].

5.10 Biometrics

Biometric technologies are increasingly being used in government and industrial applications to identify individuals, preventing the security breaches through identity theft. Biometrics typically involves using fingerprints, eye prints, facial characteristics and voice scans to identify individuals. In some cases simple biometric authentication is already available on portable devices[62]. The falling cost and increasing accuracy of biometric technologies are likely to help increase their adoption.

The widespread adoption of biometric authorisation systems could potentially reduce the need for users to manage and remember passwords for various different systems. With biometric security authorisation a user is identified by their physical characteristics rather than by knowledge that they retain (e.g. passwords). This potentially makes it more difficult for identities to be stolen.

Work on standardisation of Biometric products is being carried out by a joint technical committee (JTC1 - SC37[63]) of the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC). The European Biometrics Forum which is working on developing biometrics standards and systems is headquartered in Ireland[64].

---

[59] SSL is used to secure communications between a web browser (e.g. on a user's computer) and a web server (e.g. on an organisation's network).

[60] Pretty Good Privacy (PGP) was a widely used standard for encrypting transmitted and stored data that emerged in the early 90s.

[61] Quantum key distribution was first demonstrated by IBM in 1989. See also http://www.idquantique.com/index.html

[62] e.g. HP iPAQ h5450 - http://www.hp.com/hpinfo/newsroom/press_kits/2002/ipaq/

[63] http://www.jtc1.org/FTP/Public/JTC1/DOCREG/J1N7307.pdf

[64] http://www.eubiometricforum.com/

6 Market Development and Regulatory Issues

6.1 Market Development

With a large number of virus and hacker incidents being reported in the media users can often feel intimidated by technology. This already applies to the Internet for fixed dial-up users, but is likely to intensify as users migrate to fixed broadband and advanced mobile services. Being the victim of a computer virus or other security threats can be a costly experience for users. The loss or corruption of data, damage to hardware, loss of funds through fraud, or embarrassment (e.g. in cases where a user's identity is used to spread viruses) can cause distress to victims of computer hackers. Experience of an incident like this may make users reluctant to embrace technology, causing them to lose out on the potential benefits of communications services.

In many cases telecommunications service providers are well positioned to take on the responsibility of providing end users with more secure and easily managed ICT services. They could adopt technologies and security policies to help protect users from many of the types of security threats outlined in this document (e.g. spam, viruses, fraud), and to ensure the safety of minors.

If end users feel that security is too complex or inadequate to protect them from hackers using their resources to launch attacks or host illegal material, they may be reluctant to adopt such services. Users are typically legally responsible for data stored on their own computers and therefore they need to make sure that it is not being used illegally by hackers. Technology that can simplify the authentication process for end users so that they do not need to retain multiple identities and passwords for the various services that they use would be beneficial. The management of a unified security service could potentially be offered by third party security integration service providers.

With increasingly complex measures needed to tackle security threats and spam it is becoming more difficult for organisations to manage their own security and email systems. This can lead to greater IT costs for such organisations, and is likely to generally increase the market share of large software providers. However, savings can also be made for enterprises by outsourcing their security management alongside other IT management functions.

In the mobile area, security for 3G networks is standardised in a coherent framework by the 3GPP (Third Generation Partnership Project)[65] which aims to provide security levels that are at least equal that those on 2G (e.g. GSM) networks. Such a standardised approach will help potential users feel more comfortable with 3G security provisions. However, it will be important to maintain consistent levels of security as 3G converges with other wireless technologies (e.g. local area and personal area technologies).

6.2 Regulatory Issues

ComReg is responsible for ensuring that authorised operators are compliant with conditions attached under the Authorisations Directive (S.I. 306 of 2003)[66]. Such conditions may include ensuring personal data and privacy protection, and security

[65] See http://www.3gpp.org/TB/SA/SA3/SA3.htm for 3GPP security working group.

[66] http://www.dcmnr.gov.ie/files/CommsReg_Authorisation_final.doc

of networks against unauthorised access in accordance with national and European Community law[67]. Although ComReg has responsibilities for some consumer issues[68], the Data Protection Commissioner (http://www.dataprivacy.ie) is responsible for many general consumer security issues such as an individual user's privacy and the privacy of their data on telecommunications networks under the Data Protection and Privacy Regulations 2003 (S.I. No. 535 of 2003)[69].

A number of measures have been taken by the EU, which are related to security and privacy on telecommunications networks such as:

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [70]
- EU Council Resolution on a common approach and specific actions in the area of network and information security[71] (28th January 2003).

As well as being a general nuisance, Spam is often used as a vehicle for security attacks (see Section 4.7). Legal measures to deal with spam are generally criticized as being ineffective, and difficult to enforce. This is often due to the international nature of the Internet which enables spammers to operate from outside the jurisdiction of national anti-spam laws[72]. In some countries penalties against spammers are considered to be too low. In Ireland there is a €3000 penalty per spam message including emails and mobile text messages[73] enforced by the Data Protection Commissioner. To cope with the spam problem more effectively there is a need to tackle spammers in countries not covered by anti-spam laws. Currently ISPs are the most active prosecutors (e.g. in the US[74]). High earning spammers are often linked to organised crime and can be difficult to trace[75].

6.3 Irish Initiatives

In Ireland a number of initiatives have been set up by government and industry bodies to help protect users from, and educate them on, current security issues relating to the Internet and mobile phones. Some of these initiatives are listed below.

---

[67] See the ComReg document on conditions of general authorisations (Document 03/81) for further information - http://www.comreg.ie/_fileupload/publications/ComReg0381.pdf

[68] Note: ComReg has powers to protect users against the kind of attack described in Section 4.2 where a Software Defined Radio or other type of radio was used to cause harmful interference, provided such devices were permitted.

[69] Signed by the Minister for Communications Marine and Natural Resources on 6 November 2003

[70] OJ L 13, 19.1.2000, p. 12.

[71] OJ C 43, 16.2.2002, p. 2.

[72] The US currently produces the largest amount of spam, followed by China and Japan.

[73] See the Data Protection Commissioner's website for more details – http://www.dataprivacy.ie

[74] http://www.theregister.co.uk/content/55/36167.html

[75] "U.S. lawyers pessimistic about new federal spam laws", Total Telecom, 23 January 2004.

Computer Crime section of the Garda Bureau for Fraud Investigation deals with computer and Internet related crime[76]. See http://www.garda.ie/angarda/gbfi.html for advice on what to do if you receive offensive emails.

The Internet Advisory Board was established by the Mister for Justice, Equality and Law Reform in February 2000 to supervise the self-regulation of the Irish Internet Service Provider industry[77].

The Internet Service Providers Association of Ireland[78] was formed by Irish ISPs in 1998 and it implemented and maintains an Internet hotline to deal with child pornography on the Internet (http://www.hotline.ie), and also set up codes of practice for ISPs.

The Department of Communications Marine and Natural Resources initiated the Netsecure campaign in 2003 to help raise awareness of security issues related to the Internet[79]. Useful information and guidelines for broadband security can also be found at http://www.broadband4ireland.ie .

The Information Society Commission is an independent advisory board that is scheduled to continue reporting to the Department of the Taoiseach until the end of 2004. Useful information on the legal aspects of information technologies can be found at http://www.isc.ie/downloads/legal.pdf .

[76] http://www.garda.ie/angarda/gbfi.html

[77] IAB Report for the periods 2000 to 2002 can be found at - http://www.iab.ie/Publications/Reports/d51.PDF

[78] http://www.ispai.ie/

[79] http://www.netsecure.ie

7 Conclusion

With almost every new technology development, new security threats seem to emerge a short time later. This has always been the case with IT systems and is likely to continue where individuals seek to exploit the vulnerabilities of others.

Always-on broadband and more sophisticated mobile technologies are two key trends emerging which are likely to expose users to a new set of security threats. If these problems are not addressed quickly, potential users could be dissuaded from adopting these technologies thus inhibiting the growth of these markets. Increased awareness of these potential vulnerabilities among users can help them avoid disruption from the majority of attacks.

Although new security threats are often highly publicised in the media, most communications systems can generally be made relatively safe for the majority of users from the majority of attacks. Users need to operate their computers and other communications systems responsibly, taking simple precautions such as installing or activating security features and keeping them up to date. They need to exercise a certain amount of vigilance to help deter low tech attacks (e.g. viruses distributed through spam). Although computer security systems can often appear complex to ordinary non-technical users, they must take some responsibility to protect themselves. Users should adhere to the following basic guidelines when using computers, including advanced mobile phones, connected to the Internet:

1. Make sure built-in security features and settings are activated.
2. Keep anti-virus and other software up to date.
3. Don’t respond to any suspicious messages.
4. Don’t install or activate any unknown applications.
5. Avoid pirated software.

Security technology is developing such that the vast majority of security threats can be easily eliminated. More comprehensive security technology may be needed for users who are likely to be the target of determined high tech hackers. In such cases there is a trade off between high security and simplicity of use. Future developments in areas such as biometrics could potentially help to simplify the maintenance of security systems for end users. The benefits of a widespread adoption of broadband and advanced mobile technologies outweigh the perceived increase in security threats.

8 Annex 1 – Forward-looking Steering Panel Members

Below is a list of the members of ComReg's Forward-looking Steering Panel.

Isolde Goggin (Panel Chairperson)	Commissioner	ComReg
Eugene O'Leary	Chief Executive	TecNet
John Fagan	Operations Manager	Enterprise Ireland
Michael Donohoe	Head of Emerging Technologies	Eircom
Michael Kelly	Development Executive	TecNet
Mike Carr	Director of Enterprise Venturing	BT Exact
Paul McSweeney	Senior Account Manager	Microsoft Ireland
Philip Hargrave	Chief Scientist	Nortel Networks
Professor Gerard Parr	Professor of Telecommunications	University of Ulster
Professor Jim Norton	Independent member	
Tim Kelly	Head of Strategy and Policy	ITU

Other ComReg Members

Gary Healy	Head of Market Development	ComReg
Jonathan Evans	Technology Analyst	ComReg
Patricia Dowling	Information Officer	ComReg

9 Annex 2 - Glossary

3G	Third generation mobile
3GPP	Third generation partnership project
AES	Advanced encryption standard
DDOS	Distributed denial of service
DOS	Denial of service
DSL	Digital subscriber line
IEEE	Institute of electrical and electronic engineers
IETF	Internet engineering task force
IP	Internet Protocol
IPSec	IP security
IPv6	Internet protocol version 6
IRC	Internet relay chat
ISP	Internet service provider
LAN	Local area network
MIME	Multipurpose Internet mail extensions
NIST	National Institute of Standards and Technology (US)
P2P	Peer to peer
PDA	Personal Digital Assistant
PGP	Pretty good privacy
PKI	Public key infrastructure
PSK	pre-shared key
RADIUS	Remote access dial-in user server
RTF	Real-time firewall
SDR	Software defined radio
SIP	Session initiation protocol
SSL	Secure socket layer
TKIP	Temporal key integrity protocol
VoIP	Voice over internet protocol
VPN	Virtual private network
W3C	Worldwide web consortium
WEP	Wired equivalent privacy
Wi-Fi	Wireless local area network technology (IEEE 802.11)
WLAN	Wireless Local Area Network (Wi-Fi)
WPA	Wi-Fi protected access
XML	extensible mark-up language