International Telecommunication Union

QUESTION 9-1/2

Identification of study topics in the ITU-T and ITU-R study groups which are of particular interest to developing countries

ITU-D STUDY GROUP 2 3rd STUDY PERIOD (2002-2006)

Report on national cyberspace security infrastructure

International Telecommunication Union

THE STUDY GROUPS OF ITU-D

The ITU-D Study Groups were set up in accordance with Resolutions 2 of the World Telecommunication Development Conference (WTDC) held in Buenos Aires, Argentina, in 1994. For the period 2002-2006, Study Group 1 is entrusted with the study of seven Questions in the field of telecommunication development strategies and policies. Study Group 2 is entrusted with the study of eleven Questions in the field of development and management of telecommunication services and networks. For this period, in order to respond as quickly as possible to the concerns of developing countries, instead of being approved during the WTDC, the output of each Question is published as and when it is ready.

For further information

Please contact:

Ms Fidélia AKPO
Telecommunication Development Bureau (BDT)
ITU
Place des Nations
CH-1211 GENEVA 20
Switzerland
Telephone: +41 22 730 5439
Fax: +41 22 730 5484
E-mail: fidelia.akpo@itu.int

Placing orders for ITU publications

Please note that orders cannot be taken over the telephone. They should be sent by fax or e-mail.

ITU
Sales Service
Place des Nations
CH-1211 GENEVA 20
Switzerland
Fax: +41 22 730 5194
E-mail: sales@itu.int

The Electronic Bookshop of ITU: www.itu.int/publications

International Telecommunication Union

QUESTION 9-1/2

Identification of study topics in the ITU-T and ITU-R study grousps which are of particular interest to developing countries

ITU-D STUDY GROUP 2 3rd STUDY PERIOD (2002-2006)

Report on national cyberspace security infrastructure

International Telecommunication Union

DISCLAIMER

This report has been prepared by many volunteers from different Administrations and companies. The mention of specific companies or products does not imply any endorsement or recommendation by the ITU.

Report on national cyberspace security infrastructure

TABLE OF CONTENTS

Foreword

Five centuries ago, Galileo Galilei created an upheaval in science and technology by affirming that the book of nature is written in the language of numbers. The latest technological revolution brings us to the realization that the book of human society is written in the language of information. Zeros and ones are the bricks out of which the future is built, two symbols that constitute the entire alphabet for the most complex of phenomena: information and communication technologies.

The 1990s saw the rapid development of communication systems that made it possible to exchange information and messages electronically on a large scale, not only in the industrial and banking sectors but also for purposes of conducting online commerce and, more recently, for communications between citizens and their governments. Although priority was given at the outset to establishing and expanding networks, improving their performance and assuring their interoperability, sometimes to the detriment of security, everyone concerned with the new technologies has now come to appreciate the problems associated with them, and as a result serious consideration is now being given to the security of information and communication networks.

The potential advantages of information and communication technologies (ICTs) can only be realized if people are convinced that these technologies, including their associated networks, are safe and reliable, and cannot be misused. Establishing a stable and trusted framework of compatible standards and national agreements is a key component in building the information society and an important prerequisite to building confidence. Confidence requires, among other things, a regulatory and legal framework that is equipped to deal with cybercrime, information and communication network security, privacy protection, legal aspects of e-commerce and the safeguarding of intellectual property rights. All of these issues need to be examined from an international perspective, with the active participation of everyone concerned.

As data piracy and computer viruses grow, effective security systems need to be devised to protect information and communication networks. This requires cooperation at the international level between governments, the private sector and civil society to make it possible to coordinate the measures adopted and develop appropriate legal provisions for protecting and maintaining the security of the communication infra-structure, systems and services with which the world information society is gradually equipping us.

It should be noted that Decision 8 of the Plenipotentiary Conference (Marrakesh, 2002) set out certain action areas, one of which concerns confidentiality and security in the use of NICTs: public and private partners should not hesitate to take action if local working conditions represent a risk factor. The construction of a security environment is an important component for NICT development. Furthermore, Resolution 130 of the same conference asked ITU to engage in activities concerned with communication and information network security. Further provisions along the same lines were contained in Annex 1 to that resolution. In October 2004, the World Telecommunication Standardization Assembly (held in Florianópolis, Brazil) adopted some resolutions aimed more specifically at work on telecommunication and information network security. This report takes those important decisions into consideration and is intended as a contribution on this subject by the ITU-D working group concerned with Question 9-1/2.

1 Introduction

The information society offers immense potential for helping to achieve sustainable development, democracy, transparency, accountability and good governance. Taking full advantage of the new opportunities offered by information and communication technologies, in combination with traditional communication media and appropriate additional measures for bridging the digital divide, must lie at the core of any national or international strategy aimed at achieving the development objectives set forth in the Millennium Declaration of the United Nations General Assembly.

Among the main problems faced by governments are: data security issues; the growing complexity, breadth and scope of information technologies; the anonymity afforded by these technologies; and the internationalization of communication networks. A nation's critical infrastructures are made up of its public and private institutions in the fields of agriculture, food, water, health, emergency service provision, government, national defence, information and telecommunications, energy, transport, financial services, chemistry and postal services. The "nervous system" for all of this is to be found in **cyberspace**, comprising hundreds of thousands of servers, computers, routers, interconnected switches and information transport systems (cable, satellite, radio waves), which together enable the critical infrastructures to function harmoniously. The smooth operation of cyberspace is thus essential to the national (and international) economy, as well as to national security.

Although there is a need to ensure that every country enjoys equitable and ready access to ICTs, the fact must not be overlooked that these technologies can be used for purposes that are incompatible with the objectives of maintaining international stability and security and can do damage to government infrastructure, to the detriment of national security. Overcoming these problems will require action on several fronts at once, a determined fight against cybercrime. Securing cyberspace is a tough strategic challenge calling for a coordinated effort on the part of all players in the information society.

a) ICTs need to be made more reliable and more secure in order to bring them into wider use and increase user confidence. Particular steps that should be taken in this connection are:

   - safeguarding the confidentiality of information and protecting the interests of consumers;
   - assuring the reliability of electronic transactions and online commerce, and establishing mechanisms for overseeing this activity;
   - developing technical standards at the world and regional levels that will facilitate the establishment and use of ICTs;
   - improving the quality of world and regional networks, and assuring their continued interconnectivity and interoperability;
   - strengthening international cooperation in the fight against cybercrime;
   - devising appropriate mechanisms to publicize the importance of information and communication network security and the resources that the international community possesses in this area;
   - analysing real and potential threats to network security, with particular reference to data piracy carried out over the internet and computer viruses spread via the internet, and devising ways and means to overcome these problems;
   - improving technical information exchanges and international cooperation in the area of information and communication network security.

Sections 2 and 3 of this paper describe the resources available to ICT providers and users to protect communication and information networks, and the methods used by hackers to attack those networks.

Section 9 describes a system for monitoring data transmission, including IP, which would enable a national telecommunication regulatory agency to oversee and assure the security of communication and information networks.

b) Given the unprecedented pace at which ICTs are developing and expanding, new measures need to be taken to strengthen human rights and basic freedoms, particularly the right to freedom of speech and the right to privacy of information. This demands the following actions:

- establishing laws and regulations guaranteeing access to information and guaranteeing the public's right of access to information;
- establishing a legal framework at the national level to guarantee freedom of speech;
- applying communication and information law in cyberspace.

This subject is discussed in section 5, "Legal aspects", which takes account of the work and studies carried out by the United Nations, OECD, Council of Europe, European Union and United States, and of the corresponding reports. Following on from section 5, section 6 reports on current ISO standards, while section 7 looks at the outputs of the World Summit on the Information Society (WSIS, Geneva, December 2003) in regard to information security.

Section 8 considers the various activities carried out or under way within ITU.

An example of a data monitoring system, including the internet, is given in section 9.

Section 10 looks at relevant case studies, particularly in relation to the fight against spam.

2 Network security and protection

The notion of the telecommunication network management and protection system (security) was introduced at the global level through the ISO 9000 and ISO 14000 standards and through ISO's technical report TR 13335 "Information technology – Guidelines for the management of IT security". A network security system must be based on a set of correlated or interactive elements (political, technical, procedural, human) which together constitute:

- an approach to the management of the risks to be identified, involving the implementation and ongoing verification/maintenance/improvement of the entity's information security. In any network, account must be taken of the fact that not all of the information and information-processing systems have the same value, are subject to the same threats or have the same vulnerabilities. The process is an ongoing one in which the evolving constraints of the environment, both internal and external, must be identified and assimilated.

2.1 Concept

Businesses react in different ways when faced with a threat from hackers, but as a rule their response is to implement security measures. A security policy must be put in place and be in a position to be updated and enforced.

Instituting a security architecture involves a number of different tasks. Depending on the size of the business and the resources available to it, these tasks may be performed either by in-house personnel or by an external service provider. But these tasks are essential, regardless of who carries them out.

- Identify the project's objective, ranging from basic internet access to the development of a portal that partners can use to consult data contained in the information system.
- Identify the desired functionalities.
- Identify the resulting information flows.
- Assure a proper balance between needs and the firm's security policy (*a security policy must be implemented*).

- Determine the impact on the rest of the information system; synchronize with the managers of different functional domains.
- Identify tools or configurations that will assure the security of the information flows involved: authentication, data integrity, encryption, availability, etc.
- Select additional tools from outside sources to fulfil the requirements of the terms of reference.
- Define the security architecture with all of its constituent elements.
- Define the addressing plan.
- Establish a model for testing and validating functionalities and overall security.
- Document operating and management procedures, and establish a defence procedure for use in case of attack.
- Transfer competencies to operators and administrators.
- Establish a pilot site.
- Conduct a hacking test.
- Modify the security architecture or procedures if necessary.
- Deploy the system across multiple sites.

2.2 Technologies

Security technologies nowadays make it possible for increasingly powerful and robust equipment to be installed, often supplied in the form of specialized "black boxes" (advanced routers, switches and software).

The factors that determine the choice of solution today are cost, degree of sophistication, system administration, licensing policy and compatibility with industry standards. System administration is an important factor because the easier the interface is to handle, the more attractive the solution is. Some companies do not have a specific team dedicated solely to security, and in these cases the people responsible for the network must also look after security administration.

In addition, erecting a firewall may very quickly have an impact on subsequent choices, because as soon as a firewall is put in place it means that solutions such as authentication and encryption with the aid of VPN tunnels become more important.

As well, there are a number of other technologies that need to be used in conjunction with firewalls in order to optimize security effectiveness:

- message relay;
- antivirus software;
- proxy servers, hypertext transfer protocol (HTTP), file transfer protocol (FTP), newsgroups;
- bandwidth optimization software;
- encryption software and systems;
- log analysis systems;
- intrusion and attack detection systems;
- user authentication devices;
- "intelligent" web servers;
- tools for detecting points of vulnerability;
- caches.

In the case of connections over a wireless local area network (LAN), the connections and the data they carry cannot be altogether reliable, and so confidentiality cannot be assured without special security measures. These problems are already well known with the internet, and the solutions are fundamentally the same, involving isolation of the information system by setting up a specific "demilitarized zone" (DMZ) and establishing a higher level of security (encryption, signature, etc.). Paragraph 2.9 below discusses this in greater detail.

2.3 Routers

A router is a computer which is connected to several networks using a separate interface for each and whose function consists of conveying a data packet from one network to another on the basis of the destination address indicated in the packet's headers. By default, a router conveys all packets without exception, permits remote access (Telnet with authentication) on all interfaces for the configuration, and can be used to update software over the network as well as "remote read and write" using SNMP (simple network management protocol).

Before installing a firewall (a router that performs a filtering function, and whose routing decisions can be altered using access rules), consideration has to be given to the configuration of the next router upstream. In particular, this requires properly determining the capacity of the public network connection from the outset. Depending on how it is configured, the router connected to the network may restrict the use of certain protocols in order to prevent bandwidth congestion. This ensures that the line providing access to the internet or to a partner site will carry only those flows that have been identified as useful, and consequently thwarts any attack that takes the form of unleashing a flood of data packets. Only after this step has been completed should installation of a firewall be contemplated.

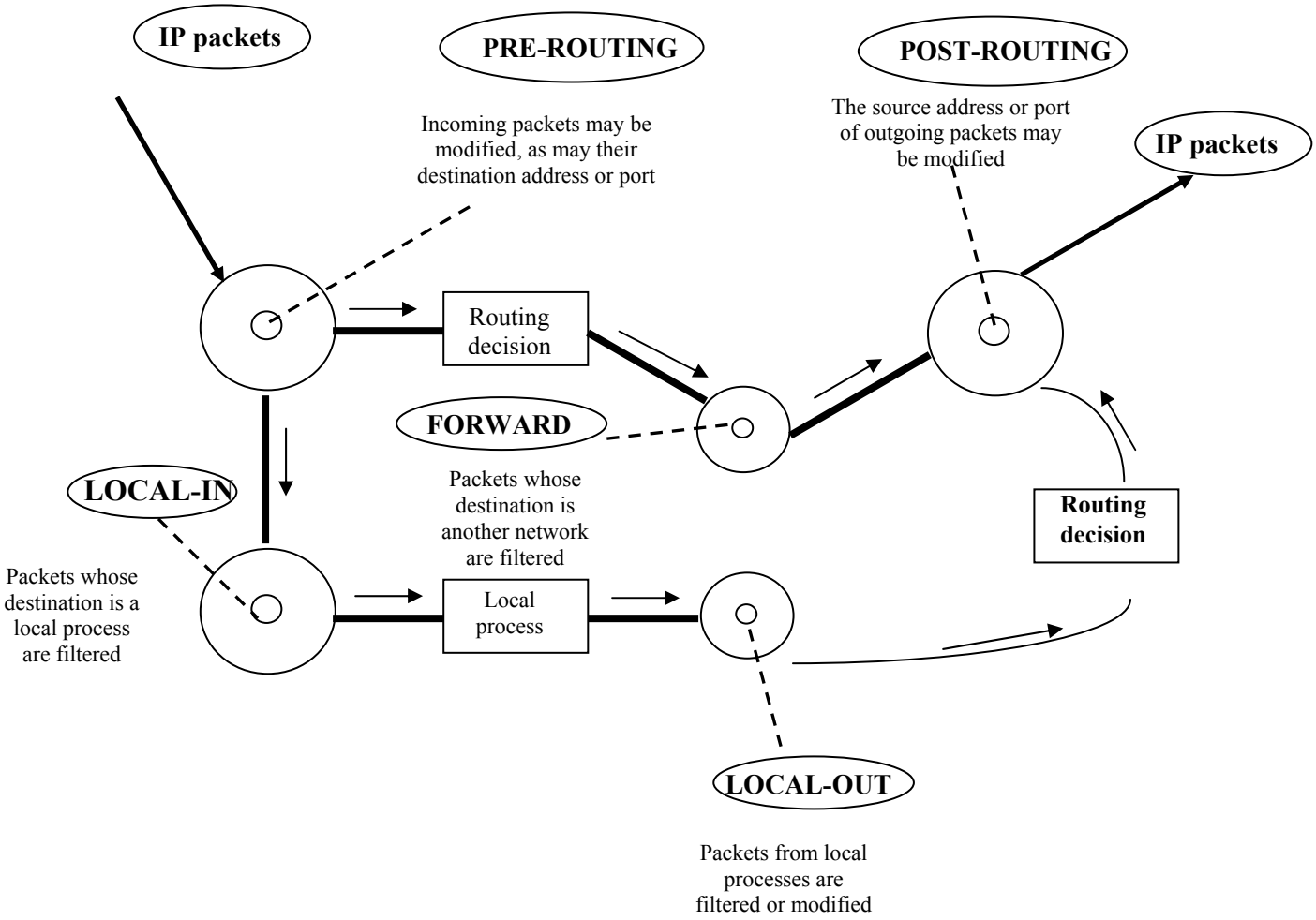
2.4 Firewalls

As a rule, the security perimeter consists of one or more firewall components, all of which have to be administered centrally. The general term "firewall" refers to a number of different software products as well as certain items of hardware that fulfil the same function, namely to isolate the corporate network selectively from other networks (incorporating defences against hackers and filtering mechanisms to thwart intruders). Accordingly, establishing a security perimeter consists of identifying the network or networks of machines and resources that are to be protected. The security perimeter is the point beyond which all incoming and outgoing connections are controlled. Authorization for a data packet to cross the firewall is defined on the basis of rules such as:

- the packet's originating address or destination address;
- the protocol used;
- the connection port.

For all the hosts situated within the protected zone, the firewall provides the sole gateway, or access point, for communications. If the network security perimeter is to be truly effective, all incoming and outgoing communications must pass through it. Consequently, the firewall plays an essential role in the solution, as it serves to guard the security perimeter. The firewall works by applying a dynamic packet filtering mechanism. It also includes a session controller and a device to analyse network layers. This means that packets are analysed at a level beyond their IP headers, and also regardless of the transport protocol used (TCP, UDP, ICMP, RPC). Each session is authorized or denied on the basis of established filtering rules. The event is logged in full detail (source and destination ports, time, date, rule number, etc.) and the information is stored in a database.

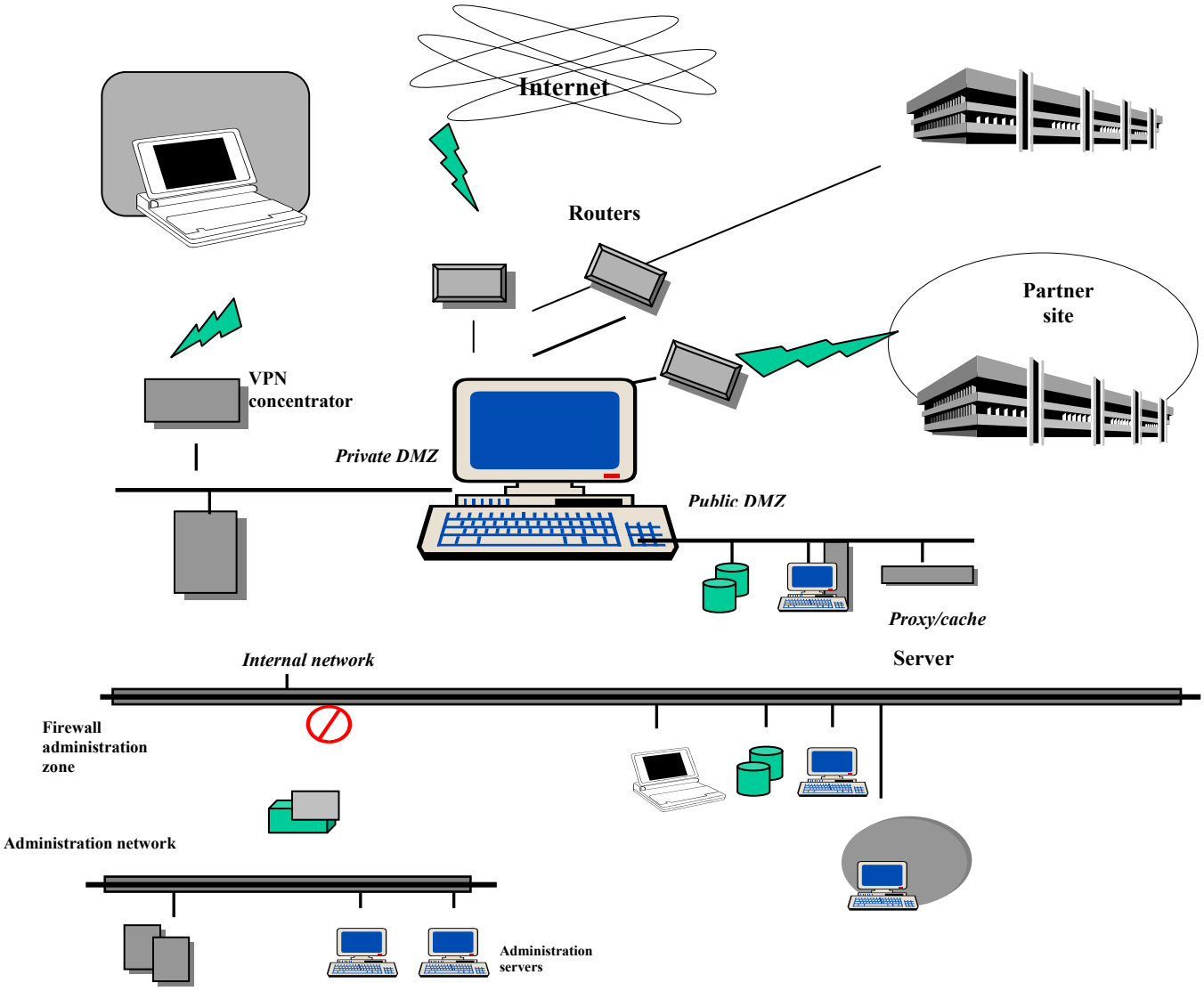
Figure 1 – Schematic diagram of a firewall



Specific attention must be given to establishing "demilitarized zones" (DMZs), or subnetworks. Most often, DMZs are set up to include equipment that is relatively sensitive or which has a specific role in the security topology used. These zones function as fully or partially watertight compartments. The various parts of the protected network use address plans that are defined on the basis of operational requirements, and which may be segmented as follows: the "access provider" network which connects to the internet, also referred to as the external network; the DMZs, of which one or more are public and one is private; and the internal network. Communication flows must be examined in detail before data are allowed to enter the security perimeter. This function is often performed by key "peripheral" components to ensure that the examination is thorough and that there is no chance that the content of the packet is malign. In addition to the functions performed by the firewall, there are also servers and items of hardware used to monitor the process and alert administrators to any abnormal situation. A firewall that is established without any of these ancillary elements can very quickly render a network vulnerable, because a firewall alone is unable to examine and analyse the actual content of data packets.

The firewall lies at the core of the network, serving as the interface between the internal network, the external network (the Web, the public network, other subnetworks), the demilitarized zones, and private subnetworks. The DMZ zone accepts connections initiated from the internal network or from the internet only for the specific services in question, while the internal service remains inaccessible from outside or from the DMZ. Figure 2 illustrates how a firewall is connected.

Figure 2 – Illustration of a firewall connection



Briefly, then, the first step in setting up a firewall is configuring it. Initially, the firewall will permit nothing to go through in any direction (incoming to the network, outgoing from the network, or access to or from the DMZ). As needed, rules will be added to permit access so that the only connections that can be established are those authorized pursuant to the security policy.

Another point to be considered in setting up a firewall is the addressing plan for the security perimeter, which has to be confidential. For this purpose, the mechanism for address translation is activated and launched on the firewall and routers so that internal network addresses are completely masked. Either static or dynamic address translation is used, as required. From an external standpoint, all IP communications use the same address in this case, or a very small number of addresses. Not only does this improve efficiency, but also, and more important, it makes it possible to authorize only those IP addresses as outgoing addresses via the internet access router.

In a case where there are two DMZ subnetworks (one public DMZ and one private DMZ, for instance), and an interface with the internal network, each subnetwork would be included within a unique range of addresses. Servers situated on the public DMZ have to be accessible from the external network (the internet). In this case, they could receive connections either directly from a routable public address or from a non-routable internal address on the internet. In the case of a non-routable internal address, a web server

situated on a DMZ would not be directly accessible from the internet. When they try to access data, web surfers will reach the firewall that has the public address of the target server on its external interface. The firewall will then translate that address into the web server's internal address, thereby giving access. In this arrangement, the firewall serves as a sort of orchestra conductor, capable of preventing all direct access to the equipment. This is the principle of address translation.

In a large network, where losing an outside connection would be a serious problem, provision is made for a certain redundancy of apparatus (parallel use of two firewalls, with one being designated as primary and the other as secondary).

It is also possible to install at least two firewalls downstream from the web switches. These switches provide for the traffic load on the access point to be shared. In this way, firewall clusters can be set up. Each cluster is independent and makes the configuration and sharing of traffic amongst the machines within it transparent to the other machines.

To be sure, such firewall clusters must always be administered centrally. A company's security policy has to be concerned with the corporate network as a whole, and the same generally applies to all the access points. If several geographic sites belonging to the same corporate network are connected to the internet, it is more efficient and more secure to perform this administration function in synchronized fashion for every case of making additions, changes and revocations of security rules. In addition, alerts are sent to one or more central consoles.

Rules for firewall security

Computer crime follows in the wake of the heavily increased use of computers in international telecommunications. Over the last years, computer crime has literally exploded, as confirmed by several international and national surveys. In the majority of countries, there are no exact figures on the number of computer break-ins or security incidents, especially those related to international telecommunications.

Most telecommunication organizations or companies do not have any specialized organization for handling Information and Communication Networks (ICN) security incidents (although they may have a general crisis team for handling crises of any type) Security incident definition is given by ISO 17799. When an ICN security incident occurs it is handled ad hoc, i.e., the person who detects an ICN security incident takes the responsibility to handle it as best as (s)he can. In some organizations the tendency is to forget and cover up ICN security incidents as they may affect production, availability and revenues.

Often, when an ICN security incident is detected, the person who detects it does not know who to report it to. This may result in the system or network's administrator deploying a workaround or quick fix just to get rid of the problem. They do not have the delegated authority, time or expertise to correct the system so that the ICN secirity incident does not recur. These are the main reasons why it is better to have a trained unit or group that can handle security incidents in a prompt and correct manner. Furthermore, many of the issues may be in areas as diverse as media relations, legal, law enforcement, market share, or financial.

When reporting or handling an incident, the use of different taxonomies leads to misunderstanding. This may, in turn, result in an ICN security incident getting neither the proper attention, nor the prompt handling, that is needed in order to stop, contain and prevent the incident from recurring. This may lead to serious consequences for the affected organization (victim).

To be able to succeed in incident handling and incident reporting, it is necessary to have an understanding of how incidents are detected, handled and resolved. By establishing a general structure for incidents (i.e., physical, administrative or organizationel, and logical incidents) it is possible to obtain a general picture of the structure and flow of an incident. A uniform terminology is the base for a common understanding of words and terms.

The ITU-T Recommendation E.409 provides an overview and framework that gives guidance for planning incident organization and security incident handling and describes the flow and the handling of an incident.

Firewalls act as guards by monitoring networks and inspecting traffic to and from the internet. Any unsolicited or otherwise suspect traffic is systematically blocked. Firewalls can also be configured so as to protect a network with respect to one or more other networks.

The five security rules for installing firewalls are listed below.

1) Identify trusted zones

The first step in protecting the network is to identify all the trusted zones. Essentially, network security in its simplest form is about trusted zones.

2) Update rules

It is very important that firewalls have up-to-date security rules. There are only two ways to verify if the firewall is really following the accepted security policy: an intrusion detection system (see paragraph 2.6 below) or a manual check, on the basis of an intrusive test or an on-firewall examination by an outside party.

3) Examine traffic log

Once the decision is taken to have a firewall security policy, it is important not to forget to record alerts in an operating log. One of the main goals of firewall management is to log all traffic. However, logging is useless unless the logs are regularly examined. This must therefore be incorporated in the rules that are part of the security policy.

4) Monitor stability

A firewall is a network infrastructure component, and as such it must be administered accordingly. This means monitoring its ability to provide the best possible running time. A firewall that is unstable will lead users to find ways of bypassing it to minimize disruption, which considerably reduces the level of security. This rule must be part of the security policy.

5) Document the security policy

The firewall security policy must be documented, to give a reference to firewall administrators and users.

An effectively documented security policy will allow users to work normally while complying with the official security policy; otherwise users will tend to react on a case-by-case basis.

The importance of a firewall (example)

Users of broadband systems connected to the internet realized just how vulnerable such systems are in August 2003, with the spread of the MSBlast worm. The worm infiltrates computers by exploiting a fault in the operating system, identifying ports that have remained open or computers that are connected to the internet for a protracted period of time. When one is found, BSBLast sets up a connection and downloads itself into the victim's computer. This becomes the new base from which the worm continues to scan the internet for other open ports in other computers, throughout the internet. In this way the worm gradually

propagates itself. The remarkable thing about this worm is that it requires no action whatsoever on the part of the user. Permanent broadband connections are thus obviously more vulnerable, although theoretically any type of connection could be affected.

In this way MSBlast infected 180 000 computers worldwide in a matter of days. Computers protected by firewalls were unaffected, firewalls helped to minimize the impact attacks. This example shows the importance of security measures such as firewalls, when one is using broadband connections. Broadband users themselves may well wait until they are actually attacked before learning their lesson and taking steps to protect themselves. However, the public authorities and ISPs could play an important educational role, and they could also take specific measures such as installing standardized security programs.

(http://www.msnbc.com/news/951168.asp?cp1=1)

2.5 Antivirus protection

There are two different sorts of antivirus protection that involve different but mutually complementary techniques.

2.5.1 Scanners

Antivirus software scans files to compare them against its table of signatures, in which the identity of each family of viruses is recorded. This is an effective technique with known viruses if the table is kept continuously up to date, but it does not provide protection against unknown viruses, or old viruses whose code has been altered.

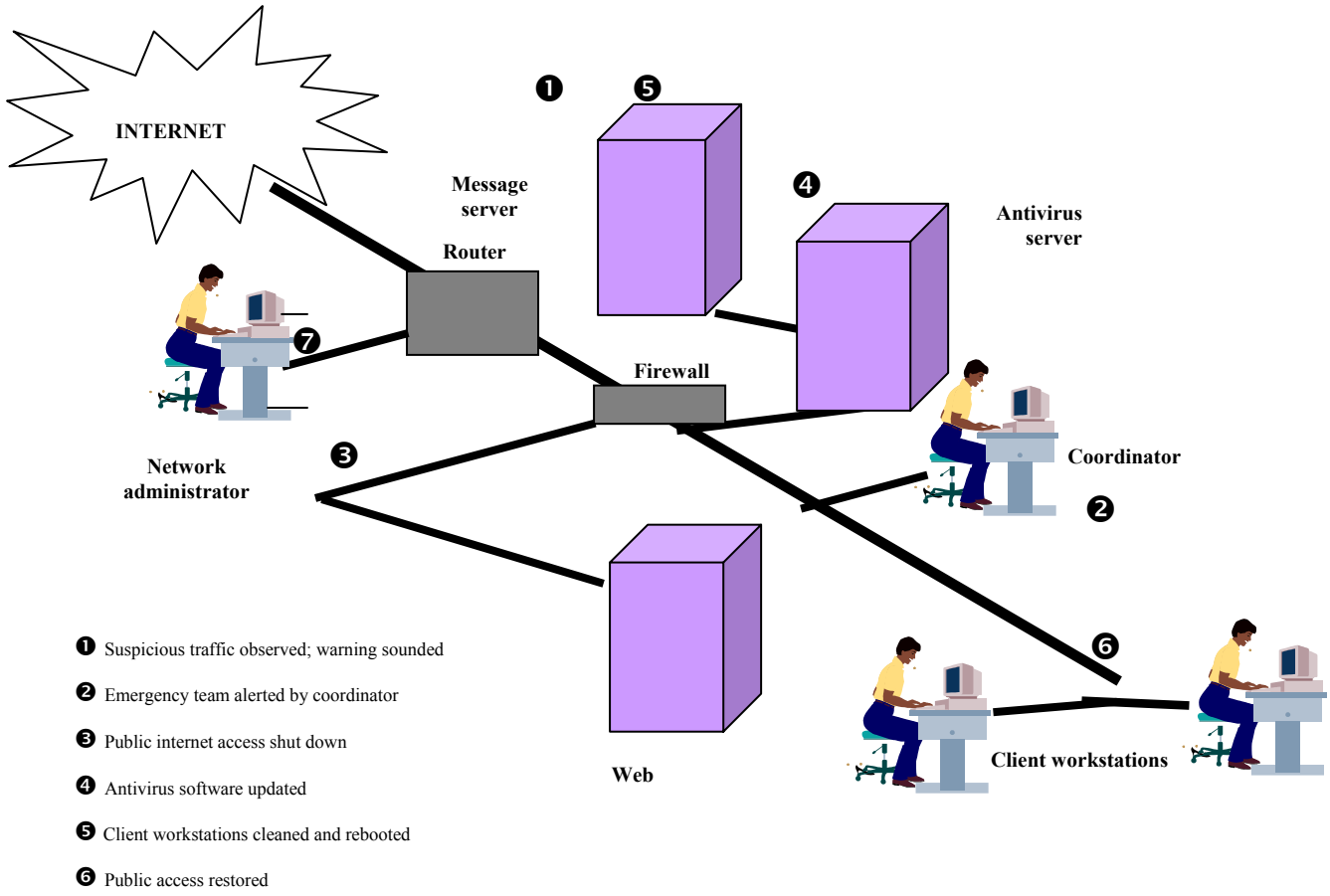
2.5.2 Generic techniques

This covers a number of different detection techniques, as part of a security policy, heuristic techniques (examination of suspicious structures in a program), verification of file integrity (detection of alterations), behaviour analysis (catching the virus in the act) and emulation of the virus in a virtual machine. Such techniques, however, are apt to produce many false alarms and to place a heavy load on the system. For that reason, they are usually used in conjunction with a table of signatures, with the heuristic engine being used only to try to intercept the most obvious unknown viruses.

As far as virus protection is concerned, corporate security policy needs to focus on two key functions: i) administration of the system and ii) coordination of antivirus security measures. The first function consists of ensuring that servers and workstations are equipped with all the necessary installations and settings to protect applications as fully as possible from virus infections. The second function requires that someone be designated as the person responsible for ensuring that antivirus protection is updated regularly. That person must also be on the lookout for virus warnings and relay the relevant information to users. When a virus attempts to propagate itself via e-mail, the person whose computer is the source of the infected e-mail should be advised. In addition, the antivirus coordinator is responsible for implementing a rapid response plan for dealing with attacks when they occur. The end-user may be taken off the network, affected applications may need to be shut down.

Just as antivirus software developers do, an entreprise should have its own rapid response centre. The emergency team should be made up of everyone directly involved. A drill should be conducted to determine each person’s proper role in responding to a virus attack. The speed with which the plan can be implemented is crucial in determining whether a virus attack can be successfully thwarted.

Figure 3 – Action plan for dealing with a virus attack



2.6 Intrusion detection systems

Intrusion detection systems (IDSs) have become one of the main concerns of businesses and operators. Many experts have pooled their efforts in an attempt to come up with a satisfactory definition of the term "intrusion", but this is not as simple as it might seem at first glance. Should simply scanning a port be considered an intrusion? And what about denial-of-service attacks which, from a purely technical standpoint, do not seek to penetrate an information system but simply to saturate it?

For the purposes of this paper, we shall define an intrusion as unusual activity within an information system. This definition includes, in particular, port scanning, direct and indirect attacks against a component of the information system, virus attacks, denial-of-service attacks, and abuses involving bandwidth utilization. The IDSs should be integrated in the security policy.

2.6.1 Categories of detection systems

2.6.1.1 Network-based intrusion detection systems (NIDSs)

NIDSs are probably the best-known detection systems. They include a component that acts as a sniffer, capturing and decoding all the packets passing through the segment to which is connected. Unlike a sniffer, however, this probe analyses IP packets in their entirety so as to identify the signatures of well-known attacks, or anomalies in packet headers.

2.6.1.2 Host-based intrusion detection systems (HIDSs)

HIDSs are software agents installed on machines to protect them, and are the natural complement to NIDSs. They have three main functions:

- detecting attacks against applications installed on the protected system;
- verifying the integrity of sensitive files;
- correlating daily files coming from applications or outside devices such as routers, firewalls and switches.

2.6.1.3 Honeypots

No doubt one of the least well-known intrusion detection tools is a honeypot, or trap, for which the inspiration was derived from military strategy. Many attack techniques use advance reconnaissance mechanisms (fingerprinting) to assess the nature of the operating systems and applications being targeted. For example, “nmap” is a fairly popular port scanner which can also be used to fingerprint a system.

As a tool for obstructing this sort of reconnaissance method, honeypots confuse scanners by emulating a virtual system and generating false responses in order to trap intruders.

The most commonly used honeypot systems are listed below:

1) Back Officer Friendly

Back Officer Friendly or BOF (www.nfr.com/products/bof) allows a Windows computer to emulate various services such as http (hypertext transfer protocol), ftp (file transfer protocol), telnet, mail, and the program back office.

With the honeypot activated, any request on the network for one of the services that are open on the machine will trigger a POP UP alarm and alert the user. Back Officer Friendly is a basic honeypot that can be used easily even by someone with limited understanding of the concept.

2) Specter

Specter (www.specter.com) is a similar honeypot with, in addition, the function of logging traffic with, and sending automatic replies to, the intruder.

This makes it more surreptitious than BOF.

3) Deception Toolkit

Deception Toolkit, or DTK (www.all.net/dtk), was one of the earliest honeypots.

This tool, with source code available on the internet, allows the user to simulate a variety of different systems offering known vulnerabilities.

4) ManTrap

ManTrap (www.recourse.com/product/ManTrap) is used to set up a number of different operating environments, above the basic operating system of the machine. The attacker sees the honeypot as separate servers with different operating systems. The tool can be used to keep a detailed track of all honeypot activity.

The chief disadvantage of these tools is related to the fact that they have a typical signature that can be identified by an experienced hacker. Since a honeypot should not be distinguishable from its environment, the best honeypots are those which most plausibly pretend to be just another server (while keeping sensitive data at a distance and remaining isolated from the other servers).

A honeypot is a security tool that can complement the existing security components. However, only organizations with a sophisticated security system already in place can afford the luxury of adding this new tool to their network architecture; this is because honeypots should only be used in conjunction with systems such as firewalls, intrusion-detecting probes, regular review of logging data, ongoing monitoring of network activity and server systems, etc.

2.6.2 Detection techniques

Various techniques are currently being used to detect intrusions, some focusing on the datagram's header and some on its data content, or payload.

2.6.2.1 Signature analysis

Most attacks use well-known character strings which can be identified within the data field: this character string constitutes the intrusion's signature. Thus, signature analysis consists basically of detecting such character strings by comparison against a library of known attack signatures and sounding an alarm when one is found.

2.6.2.2 Header analysis

Generally speaking, system reconnaissance techniques are not associated with specific character strings and therefore cannot be detected through signature analysis. Intrusions of this kind usually make use of the various parameters of IP headers, such as:

- port scanning;
- use of the TTL field to detect the presence of devices such as firewalls or routers;
- use of the fields associated with the TCP and IP options;
- hijacking of TCP flags.

Some denial-of-service attacks are very simple to implement, and exploit poor use of header parameters. One example is the so-called "land attack", which consists of using the same IP address for both the destination and the source (which is spoofed). Most communication devices do not check source addresses, so when the system being targeted receives such a request, it sends the packets back to itself until the IP stack is saturated, which can often result in blocking the system. To detect intrusions of this kind, full signature analysis must be carried out involving an analysis of the various header parameters.

2.6.2.3 Behaviour analysis

There is no doubt that behaviour analysis is the most promising area for advances in intrusion detection. Behaviour analysis consists of modelling user behaviour and developing standard profiles, so that an alarm can be sounded whenever a traffic flow outside the norm is detected. As an example, take the case of an employee at a travel agency who regularly submits requests to an airline to book tickets. Mostly, these are

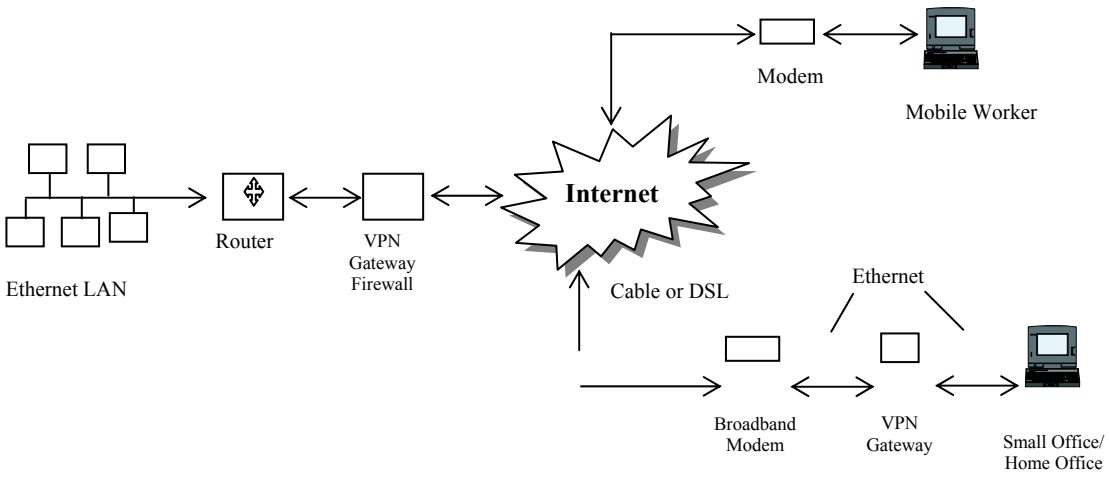
transactional exchanges consisting of relatively short packet sequences. If traffic flow monitoring detects longer packet sequences approaching the length of the Maximum Transfer Unit (MTU), this constitutes an unusual occurrence and the behaviour analysis engine sounds a warning.

Behaviour analysis utilizes inferential engines and artificial-intelligence techniques.

2.7 Virtual private networks (VPNs) and public key infrastructure (PKI)

The principle behind a VPN is to share secret information for security purposes in order to create secure connections between different devices, or between devices and client workstations. Managing shared codes becomes a problem if there are a great many devices to be administered or if the devices come from a variety of different suppliers.

Figure 4 – Example of VPN architecture



The latest generation of VPNs offers the following features:

- better and more secure internet communications, since VPNs use authentication and encryption to assure security;
- e-mail security (e-mail being a highly insecure area at present);
- improved efficiency and better communications with the company's branch offices, outside entities and remote users that connect to the system.

In a VPN with shared secret information (e.g. a network serving a country's embassies), if any one device should be compromised, then all the secret information is compromised and so is the VPN as a whole.

To keep this from happening, the architecture selected must use a public key and a private key (see paragraph 2.8). A public key infrastructure (PKI) makes it possible to administer both private and public keys.

The PKI function does not replace the management of VPN connections, but rather provides authentication keys for connections between devices on the basis of a directory (lightweight directory access protocol (LDAP), (X.509) which is common across the company and accessible to all users, and permits reliable authentication between devices or between clients and devices.

However, just as in the real world a person has only one identity, although it may take different forms, such as a birth certificate, a passport, or a driving licence, so in the virtual world there may be a need to accommodate more than one security infrastructure, giving users and applications different forms of their identity, so that each infrastructure coexists with and complements the others. VPN's should work for a given identity that could be authenticated.

Technologies like PKI and KI (Kerberos Infrastructure) can be harnessed in parallel to achieve a better result. KI was born with the Athena project at MIT; in 1999 Microsoft decided to use Kerberos version 5 in the Windows 2000 operating system, replacing the proprietary authentication protocol NTLM.

With a PKI, the need to store keys or other confidential information for a user or an application is frequently a source of added complexity for the overall architecture of the solution. A common solution (as there is no alternative offering the same level of security) is to use smart cards, card readers and equipment for storing encryption keys on servers.

Most of the systems currently using the Kerberos protocol do not require the user necessarily to have a physical card or other piece of hardware with anything private. Its utilization is therefore, as a rule, not to be recommended for applications in which non-repudiation and a digital signature are required. For this reason it is more often used for authenticating an application or user, and for providing confidentiality in a network.

However, in the viewpoint of security, the private information must be treated as securely as PKI on the user's terminal. Therefore, desirable Kerberos system should also require for storing the private information securely (for example, using secure device like smart card) on the user's terminal. And because the Kerberos server (known as KDC, Key Distribution Centre) shares private information with all of the user's terminals in most of the Kerberos systems, Kerberos system is often used in a private network.

With the introduction of the PKINIT protocol in the Kerberos set of standards, it becomes possible to use PKI authentication in a Kerberos environment. In this way the greatest benefit can be realized from the complementary nature of the two infrastructures, which form a powerful functional whole if the situation demands it.

2.8 Cryptography

Information-system security often begins with installing antivirus software to protect data and systems, a firewall to protect networks and an authentication system to protect resources.

When services such as e-commerce and e-governance are added to the mix, this requires a higher level of protection in order to create a secure space extending across networks that are vast and heterogeneous. This necessitates technologies involving encryption, authentication, stamping, acknowledgement of receipt and date-and-time stamping. The network must be made homogeneous, common methodologies issued by a trustworthy authority must be employed, and standard protocols must be adopted.

Cryptography is the science of using mathematics to encrypt and decrypt data. It makes it possible for confidential information to be made secure either for storage or for transmission over open networks such as the internet.

The first kind of encryption is encryption that uses a secret key (symmetric key). The same key is used for both encryption and decryption. If two parties, a sender and an addressee, wish to communicate securely, they must agree on a key which they do not divulge. Consequently, the key cannot be transmitted using the same channel as the encrypted message.

The problems involved in distributing keys are resolved by means of cryptography using a public key (or asymmetric key). This procedure requires a pair of keys: one public key and one private key. Anything encrypted using one of the keys can only be decrypted using the other key. Knowing one key does not make it possible to deduce the other key. Cryptography using a public key offers the advantage of enabling messages to be exchanged securely without any special device having to be installed first. The sender and the addressee do not have to share secret keys via a secure transmission channel. Communications involve only the use of public keys, and no private key needs to be communicated or shared.

Optimum security can be achieved by combining these two kinds of cryptography; this needs to be used carefully so that no false sense of security is assumed by the user. If someone wishes to send an encrypted message:

1) He creates two keys, one public and one private.

2) He retains the private key and sends the public key to his addressees.

3) He encrypts his messages using the private key that only he possesses.

4) His addressees decrypt his messages using the public key.

5) They encrypt their messages using his public key.

6) He receives their messages and decrypts them using his private key.

The must vulnerable part is the end user.

A further advantage of asymmetric cryptography is that it makes possible the use of a new functionality, the electronic signature. This enables the addressee to verify the authenticity and origin of communications and determine whether they have been received intact. Thus, digital signatures guarantee the authenticity and completeness of data: the message is hashed and the result is encrypted using the private key. They also make possible the functionality of non-repudiation, so that the sender cannot pretend that he did not send the information.

When the addressee receives the message and the signature (see Figure 5):

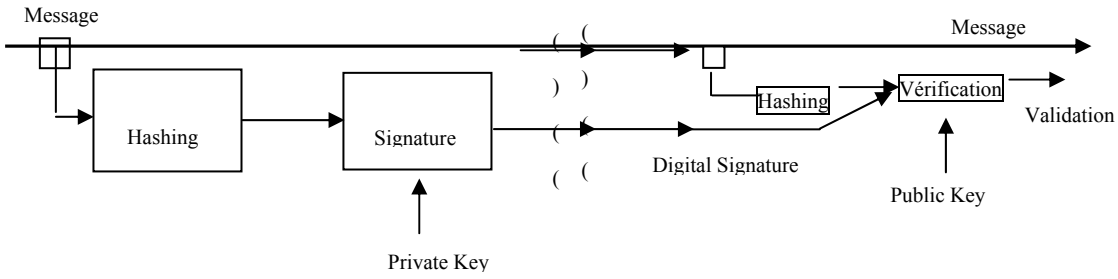
1) The message is hashed. Hashing is an opaque mathematical algorithm; the message cannot be deduced from the hash.

2) The signature is decrypted using the public key.

3) The two hashes are compared.

Someone with malicious intent could very well transmit his public key by falsifying his identity and impersonating someone else. This makes it necessary for a link to be established between a key and its rightful user, and electronic certificates fill this need. An electronic certificate is a file that makes it possible to confirm a link between an individual and his public key. Thus, systems often have to be established to handle security, records management and transfer functions. These may be in the form of relational database systems (certificate servers) or structured systems (public key infrastructure, or PKI) which handle certificate records management and administration (issuance, revocation, retrieval and records management).

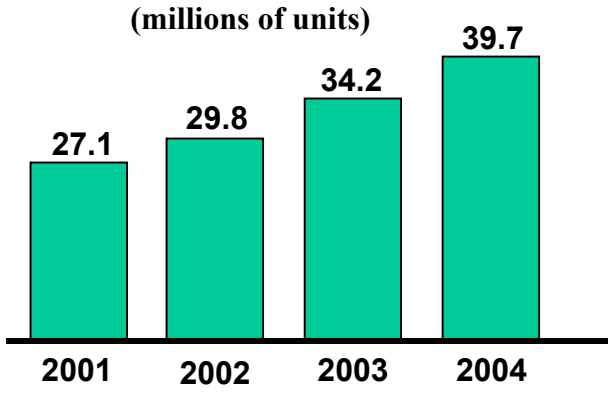
Figure 5 – Principle of an electronic signature



2.9 Wireless local area networks (WLANs)

According to the most recent information available, the global wireless network (WLAN) industry is expected to grow at an average rate of 30 per cent a year until 2006. The website <http://www.telecoms.com> estimates that the industry's revenues in 2002 totalled EUR 1.97 billion. This growth is associated with the rapid spread of portable computers both in companies and among the general public: in 2002, desktop computers accounted for 76.7 per cent of computer sales, while portable computers accounted for 23.3 per cent.

Figure 6 – Worldwide sales of portable computers



(Source: Gartner Dataquest)

Administrators of wireless networks are keenly aware of the risks posed as a result of radio coverage not being fully controlled. All the products now on the market are capable of transporting Ethernet segments, and the topologies used are similar to those of the wired world – either a station-to-station link (ad hoc mode) or a hub-and-spoke model centred on an access point through which radio packets are routed (architecture mode).

So far as small networks (those with fewer than 10 subscribers) are concerned, the network can be fully safeguarded against intrusions by using a VPN. Matters become more complicated as the WLAN is extended, for it has to be equipped with a flexible administration interface so that it can effectively control access among several subnetworks. Equipment of this kind is referred to as WLAN security gateways: these are designed to function with the access points, manage problems continuously or restore keys in the event of

cell changes, and to take credentials information from a central directory. This approach facilitates the definition of specific groups having the right to utilize WLAN connections, and avoids the awkward problem of accepting invited or temporary stations.

WLAN security

Companies which use wireless local area networks (WLANs) without taking adequate security measures leave themselves open to even the most unsophisticated hacking attacks. For the company, a breach in network security, even an apparently minor one, represents a problem. Hackers can use it to gain access to corporate passwords, connect to servers to gain illicit access to confidential information, take over a website, or even cripple the entire network.

The use of a WLAN makes it imperative for the company to set up the necessary security measures.

The simplest level of security for any WLAN is that given by Wired Equivalent Privacy (WEP).

WEP was elaborated by the Institute of Electrical and Electronics Engineers (IEEE). It is designed to a) provide basic security, b) prevent casual network eavesdropping, and c) protect the network by encrypting all data transmitted by wireless technology, using an RC4 (Ron's Code 4) algorithm that is based on a 40-bit shared encryption key.

WEP is based on shared passwords, WEP keys, which allow users to decrypt data that is moving in the wireless network in encrypted form. In actual practice, hackers can easily crack the keys by parking in front of the building, intercepting the flow of encrypted traffic using a portable computer, and deciphering it with special software that can be easily obtained from the internet. This reverse process gives the hacker the secret key, and thereby access to the corporate network.

The problem does not lie with the secret key itself, although sloppy key management makes them vulnerable to hacking. System administrators frequently assign a single key company-wide, which means that once the hacker has that key, potentially the entire corporate information repository is wide open, along with its network resources. Others provide a different key to each user, but fail to change the keys regularly. Now, a hacker who has gained access to a system will retain it indefinitely if the key environment is a static and shared one. Manual key administration is easy to implement in smaller, tightly administered networks. However, the task can become intractable as the number of WLAN users grows, frequently a sign of negligent system administration.

Security for more extended local networks requires more advanced specifications, such as automatic key changing, but it must go beyond the networks themselves, given the large number of users and the added complexity of the security constraints. Normally, larger systems require a more robust encryption key management system, authentication mechanisms, and central user management via the network infrastructure, which must not reside in the limited memory of a WLAN access point.

While WEP security, in spite of security vulnerabilities, remains localized – administered via WLAN access points – a larger system must accommodate thousands of users, along with state of the art authentication and encryption, generally requiring a centrally administered security solution. Normally these systems are administered with a RADIUS (Remote Authenticated Dial-In User Service) infrastructure. It gives centralized management and allows administration of a large number of users with authorization to access network resources.

Because RADIUS supports the 802.1x network connection standard for a wire-based Ethernet network and 802.11 for a WLAN, it offers greatly enhanced possibilities for user authentication in corporate WLANs. Given the mixed nature of the infrastructure platform in modern networks and the diversity of Windows operating systems within organizations, 802.1x emulation creates the potential for numerous, powerful and adaptive wireless security measures. The technical possibilities offered include:

- support for 802.1x network connections for existing Windows systems;
- a universal client certificate to permit mutual authentication based on certificates;
- key-protected administration, supporting RADIUS-EAP-TLS (Extensible Authentification Protocol – Transport Layer Security) protocols;
- integration in existing RADIUS environments that support the MD-5 (Message Digest 5) protocol;
- support for multiple authentication schemes with EAP protocol.

Technical solution for Wi-Fi

So far as experience in making the operation of corporate Wi-Fi networks both viable and trustworthy is concerned, a technical solution known as "wireless switching" is now being applied. This innovative approach consists in moving all of the network's administrative functions (radio parameters, security, connectivity with the wired network) into a dedicated switch, thereby "lightening" the access points and centralizing the management of the Wi-Fi infrastructure.

Unlike a traditional Ethernet switch, a Wi-Fi switch natively manages the IEEE 802.11 traffic received from the access points connected to it (in reality, simple WiFi/Ethernet bridges). This gives it full control over the wireless network.

In this model, network administrators have access to a unique configuration interface that affords them global visibility vis-à-vis the network and its users, and which they are able to administer in the same way as the company's existing wired network: authentication using a RADIUS, LDAP or even Active Directory service (which permits re-use of the Windows domain user accounts for monitoring network access), monitoring of user bandwidth consumption, DHCP (dynamic host configuration protocol) dynamic network configuration, etc.

By adopting the Wi-Fi switch solution, the administration team can effectively protect against specific threats to wireless networks:

– Access point intrusion (deactivation by deauthentication, i.e. the transmission of instructions which prevent users from authenticating themselves at the terminal): automatic detection and sending of disconnection packets to all clients in order to ensure their protection.

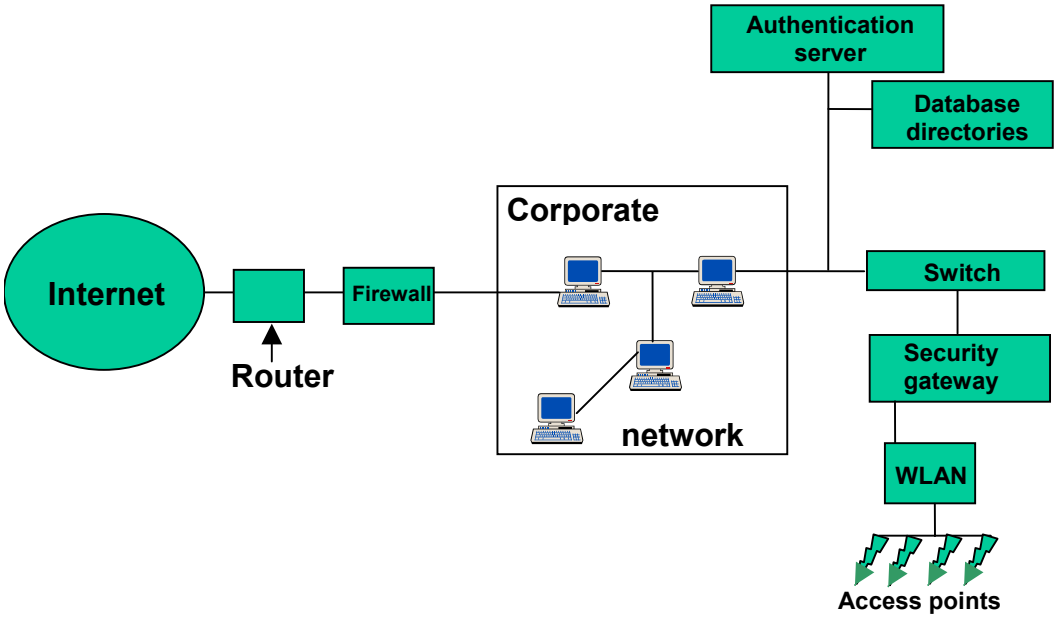
– Denial of service (flood): monitoring the frequency of network management operations.

– Masquerading (man in the middle): detection of Wi-Fi address spoofing.

– Passive eavesdropping (sniffers): the equipment used takes the fingerprint of the passive eavesdropping tools and throws them out of the network.

Whatever level and scope of wireless security a network infrastructure may require, a layered solution can be customized to meet specific needs. Wireless security solutions range from simple WEP, based on standards, to security managed at the access points, with robust and adaptive centrally managed security, and from wire-based to wireless infrastructure.

Figure 7 – WLAN security layout

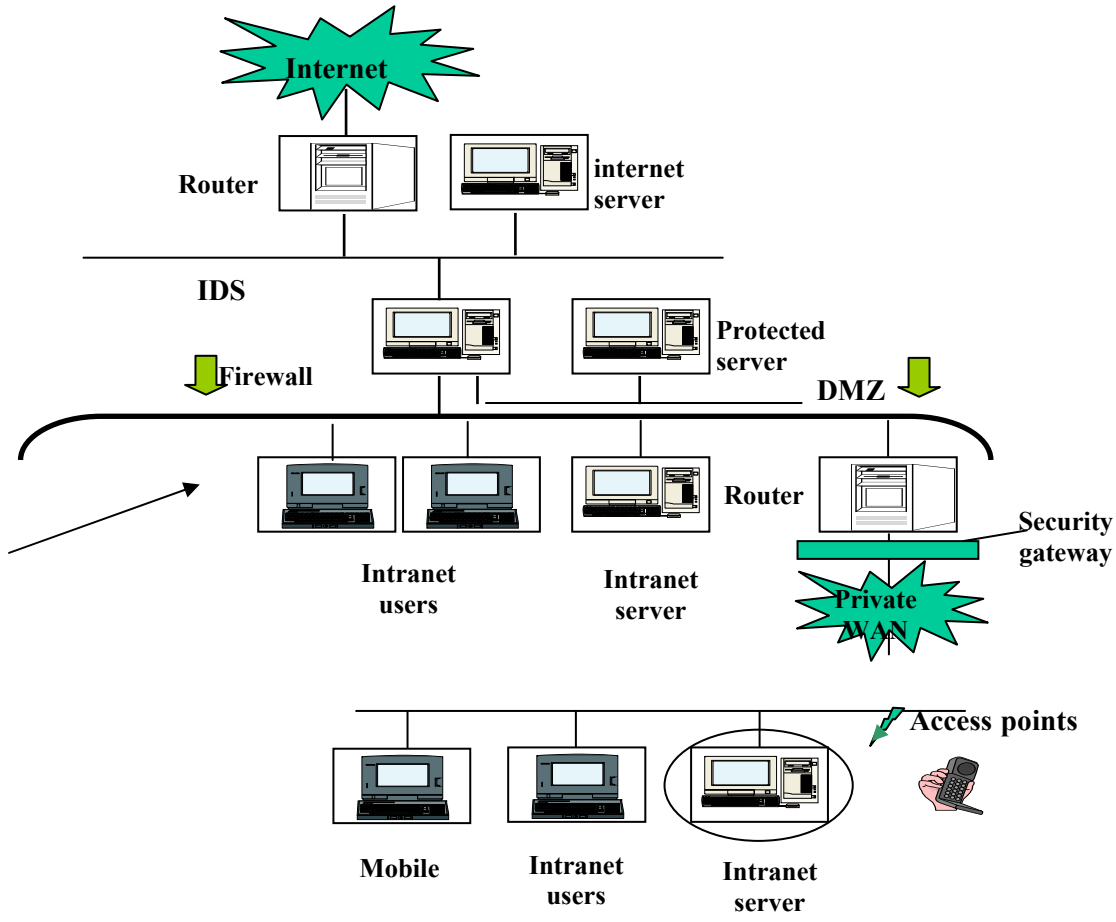


NOTE – For data storage purposes, many laptop owners use a USB (universal serial bus) stick, i.e. a flash memory which operates like a removable hard disk and has a capacity ranging from 32 to 512 MB. Numerous manufacturers supply USB sticks with security software that enables users, by means of a password, to protect their data in the event of loss or theft.

2.10 Review

In the foregoing paragraphs, we have described the main methods used to make a communication and information network secure and presented a security approach geared in particular to dealing with the risks associated with the new ICTs. Figure 8 below shows what a network security layout might look like.

Figure 8 – Schematic network security diagram



3 Intrusions; automated attacks

The devices and software described in section 2 above are designed to safeguard communication and tele-communication networks which are vulnerable because they are connected to the internet. Every electronic message and every file transmitted via the network is handled by these devices. The tools and methods currently used by hackers to mount attacks against networks are described below.

3.1 Viruses

Viruses of many different kinds – viruses within executable files, macro viruses, script viruses and sophisticated worms – exploit security weaknesses in operating systems in order to propagate themselves over networks (see Figure 9).

According to the broadest definition, a computer virus is a self-replicating program: in other words, it generates copies of itself within existing files.

Viruses are characterized on the basis of how they reproduce and infect a computer – focusing on the boot sector, on application files or on executable files – rather than the effects they produce. They may do a wide range of damage: create a message, erase files, format a disk, flash the CMOS memory, or even install a "Trojan horse" (a Trojan horse is a program that sits on a computer and waits to open a security breach such as a "time bomb", backdoors, or spyware). A virus conceals a malicious function within a file that appears to be sound.

The earliest known viruses date from the late 1980s. They would install themselves in the boot sector of diskettes and hard disks and would infect any new diskette inserted into the computer. Soon, other viruses came along that could infect PCs by contaminating executable files. A single program might be contaminated over and over again, with the result that its file size would keep growing and growing. Virus programmers then started using existing viruses and making more effective versions of them. Consequently, the second generation of executable-file viruses was more advanced and would not reinfect files that had already been contaminated.

The proliferation of viruses is closely associated with operating system security. In Windows systems, any user can modify any of the system files, including executable files, with no restriction whatsoever. Even recent professional-level operating systems such as Windows NT and Windows 2000 do not apply a real file security policy unless they use the NTFS (New Technology File System) format which allows attributes to be defined for each file. Moreover, many users log on in administrator mode, which makes security breaches more likely to occur. It is fairly easy for an executable virus to spread on a system of this kind, unlike the situation with system files. Nevertheless, there are specific attacks targeted on Unix, and worms targeted on Linux or Solaris. These virus programs exploit specific network security weaknesses to gain access to the root account and contaminate the system.

3.1.1 Multipartite and polymorphic viruses

In 1996, a new generation of viruses began to appear, known as macroviruses. Initially, macroviruses were used to automate a number of tasks. There are even multipartite viruses that pass from one Office application to another. Polymorphic viruses contain a special code that makes each infection different from the previous one. These viruses incorporate a specific code that alters their signature so that they cannot be identified. A polymorphic virus can assume millions of different forms.

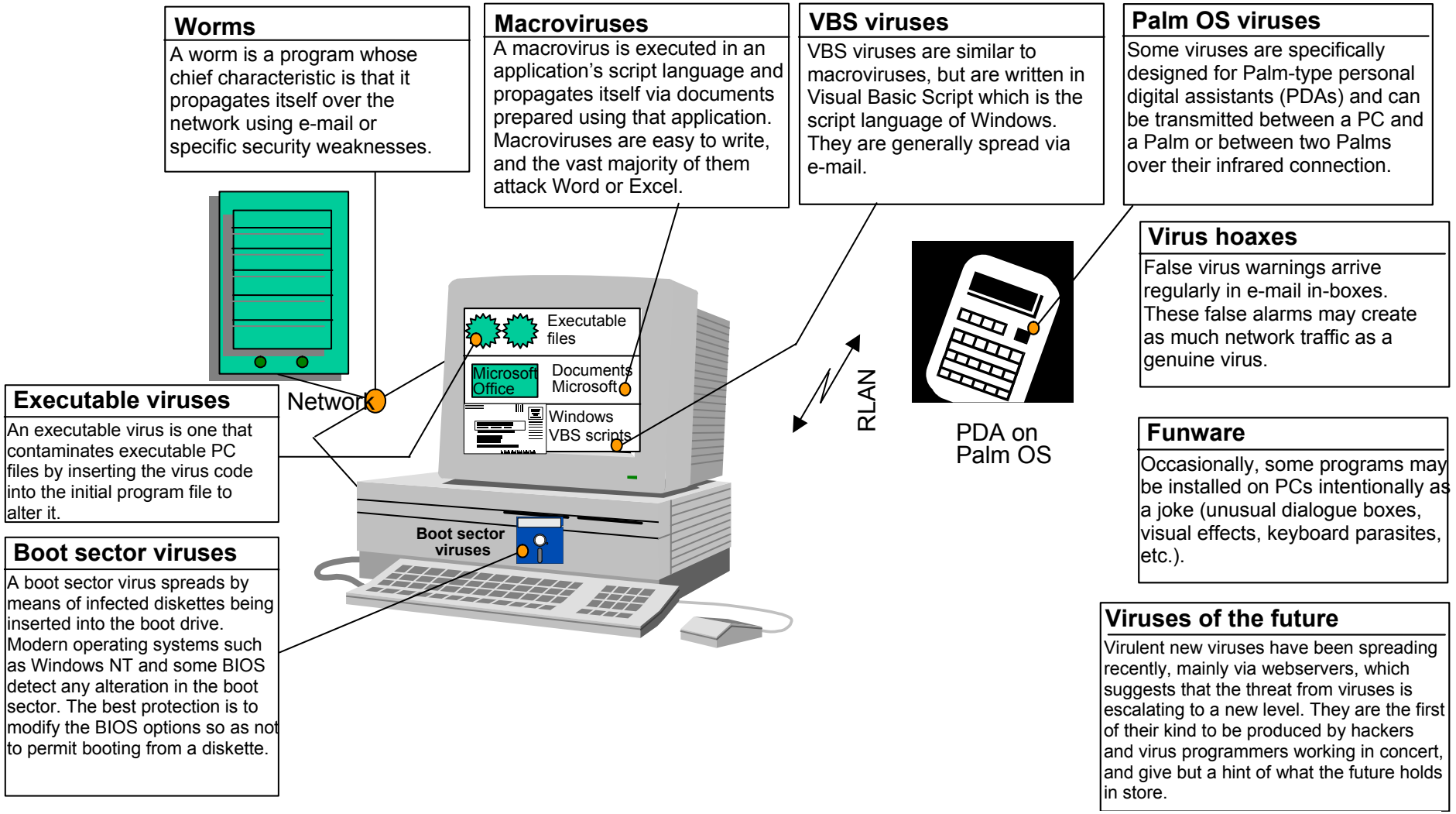
Before the advent of macroviruses, only specialists who were expert machine-language programmers were capable of creating a virus. Using advanced programming languages, however, programming a macrovirus is relatively simple once the basic concepts are understood, and creating a variant or "mutant" using a specimen of an existing virus is very easy indeed. (Although a new variant of a known virus is referred to as a mutant, a virus is unable to mutate on its own; any mutation must be created by a programmer.) Over 95 per cent of the viruses in circulation today are macroviruses. They take advantage of easy network and e-mail access using Office applications.

In the autumn of 2000, a new kind of computer bug started to appear: script viruses written only in Visual Basic Script (VBS). This feature distinguishes them from macroviruses. As well, they affect only Windows system files.

Since 2001, there has been a resurgence of executable viruses. Recent mutants have become very complex programs and use hackers' techniques to penetrate systems and propagate themselves.

Figure 9 below describes the different types of viruses that can affect a communication network.

Figure 9 – Different types of viruses



3.1.2 Malware – the virus threat of tomorrow

The explosive growth in communication infrastructures, the widespread availability of broadband, and broad acceptance of internet-based exchanges have all contributed to breaking down the limits on the size of e-mail messages, attachments, and other downloaded files.

This has brought about a revolution in computer viruses (including worms, Trojan horses and other malicious code), which, in a period of a few years, have become sophisticated software packages with a whole range of specific functions.

This new generation of virus, which should be known by the generic term of malware, displays a level of technological sophistication that makes it clear that the current and future threat will be an order of magnitude beyond what has been known hitherto.

Viral functions utilized

To fully understand this situation, it is important to understand some of the more common viral functions.

- Downloading and installation of automatic hacking tools. For example, *HackTool/Scansql.A* runs a known, legitimate tool for finding passwords authorizing access to MS SQL (Microsoft Structured Query Language) servers using a simple text file as a test password list.

  If the passwords consist of names, or common words – which is the case in 80 per cent of the cases – the search result becomes automatically available for the next worm, hacker or malicious user.

- Remote takeover of a computer.

  Trojan horses like *W32.Sobig* make it possible to take over a computer remotely and run a program or any command.

- Collection and automatic retrieval of keystroke loggers by SMTP (simple mail transfer protocol) or FTP (file transfer protocol).

  Worms and Trojan horses such as *W32/lovgate* are very significant, through their technical evolution and the variety of processes that are triggered.

  This type of virus combines, for the first time, all of the above functions, in addition to opening a backdoor that leaves the computer open to infection even after the initial virus has been removed. Furthermore, the form of compression used allows it to be executed directly, from the "preview" stage of the mail program, without requiring any preliminary decompression.

- Creation of a special SMTP server on the infected computer to spread the virus.

- Continuous creation of domains on remote servers.

- Extraction of the contents of all e-mail address books on the computer for use by the malware SMTP server.

- DoS attacks against mail servers and nearly instant exploitation of new security vulnerabilities.

- Copying of IP (Internet Protocol) addresses of computers by connecting to the access provider, using the mail program addresses.

- Modification of the automatic signature in the mail program to ensure dissemination with each outgoing e-mail; installation of new favourites or shortcuts in the web browser; addition of new toolbar buttons; modification of the start page that comes up automatically when the browser is opened.

The *Js/Fortnight* worm, among others, uses this method to spread and, in particular, to re-contaminate PCs automatically by downloading its code when the internet is accessed.

As the complexity and the magnitude of the threat grows, increasingly heavy administration tools, such as SQL databases, are being brought into use for the sole purpose of managing virus alerts.

An extremely worrying development is that, as the attacker community improves its knowledge of operating systems, new vulnerabilities are constantly being discovered, and then expertly targeted almost immediately.

Conclusion

The threat of computer viruses makes business security an urgent matter. How crucial this is, may be judged from the increasing rapidity with which viruses have been propagating themselves as their character has evolved, since the 1990s.

At the start of the 1990s, the time to react to a file virus was in the order of one month; by the end that decade, e-mail viruses demanded a reaction within an hour. It is clear that, in the near future, so-called flash threats will see malicious code doing its damage in a second.

The possibilities include automatic BIOS flashing when a computer session is closed, changing the start track of a hard disk, automatic formatting, overwriting executables to turn them into viruses, widespread modification of network user profiles, etc.

All of these technical possibilities exist, but they are not easy to implement in current software languages without being detected. However, it is no longer inconceivable to develop a separate language with its own compiler; this shows where future threats may come from.

Managing the risk from viruses is an increasingly complex task, with new viruses requiring a growing number of layered defences, even at the level of the operating system, which must be able to protect itself. It is indicative of the situation that Windows XP is now delivered with a firewall of its own, at the workstation level.

Network and business security against computer viruses of all kinds remains a matter for the experts, because of the need to continually follow technical developments and keep up with virus evolution, which is limited only by the imagination of malware authors.

3.2 Evasion and insertion techniques

The more popular intrusion detection systems (IDSs) become, the harder hackers work to develop new ways to detect the detection systems. These techniques, which seek to prevent an IDS (see paragraph 2.6 above) from sounding an alarm, fall into two categories.

3.2.1 Evasion techniques

These consist of disguising the attack sequence in such a way that it will be correctly interpreted by the targeted system but not by the IDS.

The web server being attacked will automatically delete any excess characters, so the IDS will see a different character string and will not sound the alarm. Some IDSs are able to detect this kind of evasion technique, but this is not systematic and it is something that needs to be checked as part of a technical validation.

More advanced evasion techniques make use of polymorphic codes.

3.2.2 Insertion techniques

These consist of inserting into the signature character strings that will be decoded by the IDS, but not by the machine being targeted. A common method is to cut up the signature and insert additional fragments to create a TCP header checksum error.

Indeed, few IDSs currently available on the market perform checks in this area (mainly for performance reasons), so the parasitic sequence will be inserted into the attack sequence. So far as the machine being targeted is concerned, however, the fragment that has been inserted will automatically be deleted by the TCP/IP stack that makes the necessary checksum checks.

3.3 Denial of service

3.3.1 Denial of service

Denial-of-service (DoS) attacks are a common and recurring concern in the world of networks and their security infrastructure. By preventing both incoming and outgoing internet access, DoS attacks can sow chaos in a company's ability to manage its online business, as well as in its relations with customers and shareholders. Even a shutdown of information systems that lasts only a few hours can deal a serious blow to the company's reputation and erode customer loyalty.

Traditional DoS attacks are designed to make a computer or network crash by saturating it with a huge volume of traffic using TCP (transmission control protocol), UDP (user datagram protocol) or ICMP (internet control message protocol) data packets.

Individually, these packets appear harmless enough, which makes it easy for them to travel through a company's firewalls and routers. Disguised as normal traffic or as traffic coming from the equipment manufacturer, these packets are often exempted from the controls to which each package would normally be subjected.

3.3.2 Distributed denial of service

A distributed-denial-of-service (DDoS) attack is more sophisticated than a DoS attack, and it is becoming increasingly popular amongst hackers.

A DDoS attack makes use of many machines connected to the internet. Once a large number of systems have been compromised, they are used collectively to launch a torrent of distributed attacks against a single target site. This is done by loading a software program on all the various machines that have been compromised, located in a number of corporate and institutional networks.

Hackers seem to prefer university networks as a launching pad for DDoS attacks, since applications are shared widely in such a setting. Once the software to be used has been installed on hundreds of machines, the attacker can activate them all remotely.

4 Network protection principles

4.1 Organization

Within the administration or company, responsibility for security should be shared between an information system security officer (ISSO) and a security operation centre (SOC).

The ISSO unit should report directly to a top executive in order to define a security policy that is appropriate for the needs, the professional structure, and the objectives of the organization.

The ISSO must make WLANs part of the security awareness campaign to educate users about the risks associated with WLANs; the objective is that they should report to the security service every time a wireless connection is made without proper authentication.

An important part of the ISSO's work is to establish a security policy and associated procedures that take WLAN issues into account. It should be noted that ISO 17799 does not deal with WLANs at all. (See section 5.)

The SOC should be part of the IT branch, like the IT service that manages central servers or the office technology service that is responsible for managing PCs and desktops.

The responsibilities of the SOC are first, to manage the components of the information system, security being the principal objective, and second, bring an overall security perspective to the entire information system (a wireless access point is always at the perimeter of a network; for this reason, like all such peripherals, it should be managed by the SOC). These centralized functions are, in particular, based on analysis and correlation of logged data and intrusion detection.

These constituents of the information system, having security as the main objective, consist primarily of all the means of interconnecting with the outside world, which are to be found on the organization's perimeter for internet access, the VPN (virtual private network) for remote access, extranets, and e-commerce platforms. These systems should be operationally managed by a dedicated security-oriented service. The same applies to user authentication, for example for remote access or access via internet.

4.2 Finding the origin of a security incident

Monitoring the activities of all components of the information system is essential at each stage in the effort to track down an incident. The objective of monitoring is to track (for the network as a whole but also within the individual elements of the information system) the activity that is generated by a malicious person and to issue an alert if others attempt to exploit the same vulnerability for a malicious purpose, but also to provide a view generally of the scope of the incident.

Monitoring should focus on network traffic (date and time of activity, volume of data exchanged, origin and destination) but also on activity within the elements of the information system (CPU workload, memory used on a server, changes to binary programs, creation or deletion of server data, etc.).

Network monitoring components should be installed in very specific parts of the network. The assumption is that they are protected from being compromised, particularly as regards the integrity of log files. Monitoring the activity of system elements relies mainly on performance tools (Patrol, HP Open View, etc.) and log files.

It is important at this stage to ensure that the clocks of all the various components of the information system are synchronized, for ease of event correlation. One of the techniques for monitoring information systems is to conduct a broad monitoring campaign to identify the perimeter that needs to be covered, along with a narrower activity that focuses on the components that are actually affected by the incident (analysis of an individual service or user account, for example).

Restoring the information system

The objective of this phase is to restore the information system in such a way as to undo the incident and prevent a recurrence. It can only be initiated once the incident has been fully analysed, with identification of the attackers and their operating methods (Trojan horses, user accounts etc.).

The level of rights obtained by the attackers gives an indication of what actions they might have performed. The location of the compromised component within the network (with respect to the network topology but also its situation within the trusted domain between components) may point to other components which need to be included in the perimeter of what has to be restored.

If all of the operating methods used by the attackers have been identified, then the components can be restored on the basis of just those vulnerabilities that have in fact been exploited. If doubtful areas remain, it is recommended to restore the components using the original manufacturer's CD ROMs. Restoring from backups is not always a good idea, unless one is absolutely certain that a particular incident occurred after a particular backup; otherwise, restoring from a backup will only succeed in restoring the Trojan horse or other vulnerability. Once restoring has been successfully performed, the compromised components need to be hardened and the vulnerabilities eliminated.

Naturally, the entire procedure of restoring the affected components is not done directly with the network on line. It is only once the components have been restored that operation can be resumed and the connection to the corporate intranet restored. Many organizations adapt their security level in response to the incidents that occur. It is in this phase, therefore, that new security resources can be put in place, such as a modified network topology, access control lists, beefed-up integrity checks, updated user lists, a revised security policy, or a user awareness campaign. Naturally, it may not be possible to implement all of these measures in the days immediately following an incident; what is essential is that the ISSO should set up a formal action plan that may spread across several months or even years.

Formalization

All of the actions taken as part of the response to a security incident must be formalized and compiled into a file for subsequent analysis. Once the urgency of the situation has passed, this documentation can be used to run the same tests again, determine whether technical evidence may have been destroyed by investigators in error, review any conclusions that may have been drawn, collect technical evidence on the incident (or a suspect) in the event of a disciplinary or legal procedure. Dealing with all of the ramifications may take several months, and during that time it becomes very difficult to keep track of all the actions undertaken unless they have been systematically recorded from the outset. The importance of the formalization stage should thus be evident.

It should always be remembered that an attacker may have infected the network with a variety of means, along with detectors that will alert him or her of imminent detection. All electronic exchanges, technical evidence that has been gathered, incident reports and so on must be recorded outside the information system. It is not at all rare for an attacker to observe the detection and response efforts by monitoring this information, allowing him or her to selectively destroy data or technical evidence. A report of the type described above can be used ultimately to propose new protection measures for the information system and to raise the overall security level of the organization.

Conclusion

Compiling the technical evidence after an incident is no simple matter. Only by taking very precise steps and following a methodology such as that described above can an airtight procedure be framed to prevent an attacker from succeeding with a second surprise attack, and minimize the risk that a security incident will escalate into a full-blown disaster.

4.3 Integrated cyberspace security solutions

Security must be incorporated in every domain of the information and new-technology society. Every link in the information chain must be aware of the security problem and participate in setting up **integrated solutions**.

An overall solution for cyberspace security has to take everything into account, from an overall risk analysis to the integration of optimum solutions, from low-cost developments to total security management:

1) Analyse: consultation and services in security risk management

- Analyse and assess risks (technical, legal, human etc.)
- Technical and functional security audits (ISO, ITU etc.)
- Vulnerability and intrusion tests; identification of weak spots
- Organization of security management
- Security policy and master plan, including active security monitoring
- Security education and awareness training
- Emergency IT assistance, follow-up, emergency response

2) Select and deploy: implementing and deploying security

Selection: Architecture validation, pilot assessment, technology selection, solutions

Deployment: Implement and integrate the solutions, provide project management, make it operational

In summary:

- Propose solutions that are integrated or adapted to:
  - guarantee security of networks and infrastructure in use
  - ensure secure connectivity for mobile users
  - protect identity management and critical data
  - guarantee digital confidence for exchanges
- Construct sustainable, upgradeable architectures
- Provide stringent supervision and project management
- Deploy the security system – technical and human aspects alike

3) Control and sustain: global security administration

Control: administer, supervise, operate, maintain and modify the deployed systems (incorporation of new technologies)

Sustain: maintain, control, actively monitor, update, adapt security policy

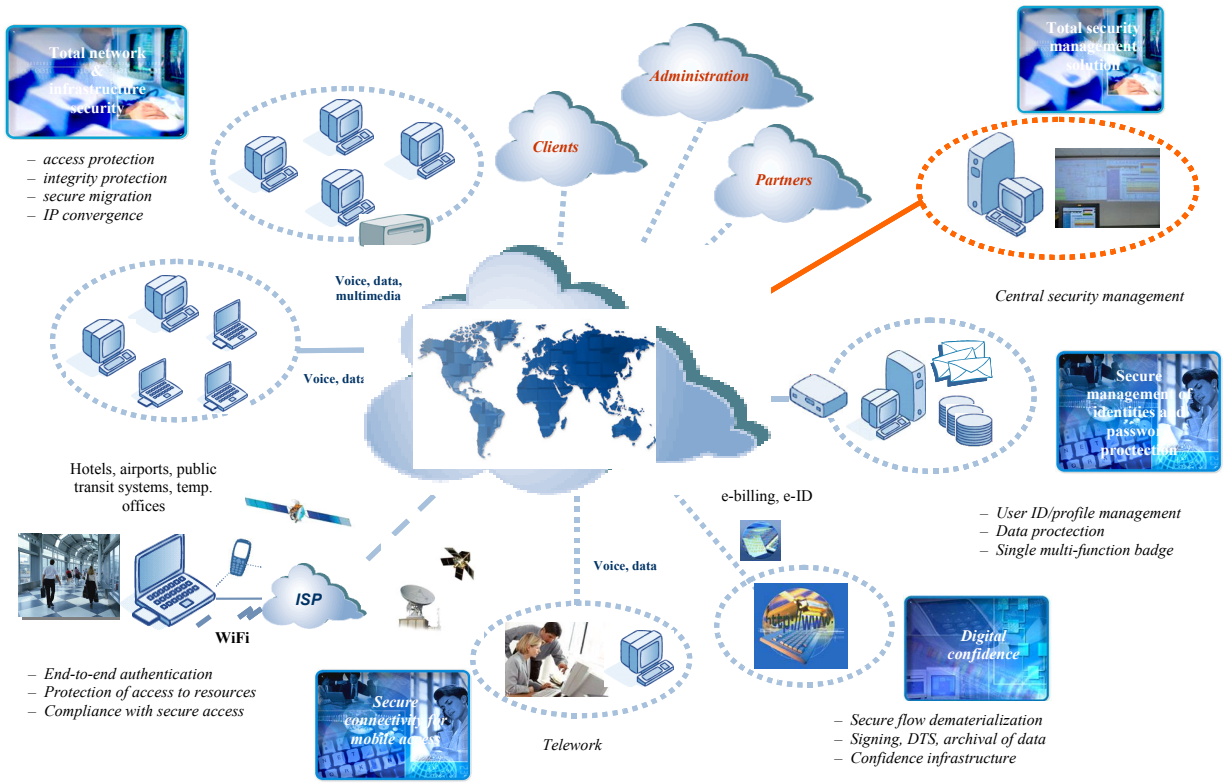
In summary: permanent assistance/support and active supervision

- Remote administration
  - Safe remote security and administration solutions (COTS)

- Anti-virus team
  - Pro-active monitoring, preventive and reactive action
- Security management for fixed and mobile workstations
  - Administering rights, verifying security level compliance
- Secure hosting
  - Structure and DTS logging
  - Trusted infrastructures (PKI)

The figure below provides a partial overview of the various components of an integrated security solution.

Figure 10 – Integrated security solution



5 Legal aspects (cybercrime)

The rapid development of information technology has had direct repercussions on all segments of modern society. By making it possible to store all sorts of data and to transmit those data over long distances, the convergence of telecommunication and information systems has opened up a wealth of new possibilities. These advances have been supported by the advent of information networks and "superhighways", particularly the internet, thanks to which practically anyone, anywhere in the world, can have access to the full panoply of electronic information services. By connecting to communication and information services, users create a sort of common area, known as "cyberspace", which although it serves legitimate purposes can also lend itself to abuses. The offences that can be committed in cyberspace may be against the integrity, availability and confidentiality of computer systems and telecommunication networks, as well as classic offences that simply make use of cyberspace as a new tool to aid in committing them. Although such

offences may be international in character (offences perpetrated over the internet, for instance), enforcement agencies typically have a national focus. Increasingly, cybercriminals are ensconced in safe havens far removed from the locations where the effects of their actions are felt. As a rule, a country's laws apply only within the territory of that particular country. And so the solution to these problems has to be found in international law, which makes it necessary for appropriate international legal instruments to be adopted. Criminal law has to keep pace with technological progress, which provides highly sophisticated means of using cyberspace for malicious purposes and thereby threatening legitimate interests. Since information networks pay no heed to borders, a concerted international effort is essential to deal with such abuses.

On the other hand, attempts are being made in some areas to protect public areas against technology-induced disturbances.

Thus, in France a law was passed in July 2001 that allows mobile communications signals to be jammed in performing arts centres, cinemas and correctional facilities. The latter, in particular, have seen jamming since 2003, for security reasons. In October 2004 the French minister responsible for telecommunication signed the law authorizing similar measures for the performing arts centres and cinemas.

There are three types of technology available. The most radical method, broadband jamming, involves continuous transmission on the telephone relay frequencies. The least intrusive method makes use of repeaters to allow emergency calls from cell phones while blocking incoming calls. This should be the preferred solution for cinemas and theatres.

Between those two extremes, there is jamming in the proper sense of the word. Jamming systems block communication between the cell phone and the operator's relay by transmitting a parasite signal, regardless of the origin of the communication, but only when a call is detected. This is the system that is used in correctional facilities.

5.1 Guidelines established by the United Nations and by the Organisation for Economic Co-operation and Development (OECD)

As early as 1994, the United Nations focused on the problem of cybercrime by publishing a manual on the prevention and control of computer-related crime. That manual was updated in 1997, and since then the United Nations has adopted security guidelines for information and communication systems. The Organisation for Economic Co-operation and Development has also adopted guidelines for the security of information systems, based on the following nine principles:

1) Awareness

   Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

2) Responsibility

   All participants are responsible for the security of information systems and networks.

3) Response

   Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents.

4) Ethics

   Participants should respect the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

6) Risk assessment

Participants should conduct risk assessments.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

8) Security management

Participants should adopt a comprehensive approach to security management.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

Subsequently, in August 2002, OECD published a document entitled "OECD Guidelines for the security of information systems and networks: towards a culture of security". These guidelines, which concern all players in the information society, highlight the need for a better understanding of security issues and advocate the development of a "culture of security". Indeed, security should be a key concern during the development of systems and networks, to which end new ways of thinking and behaving need to be adopted in respect both of the use of information systems and networks and of the exchanges for which they are used. The guidelines constitute a foundation for work towards a culture of security throughout society.

The OECD Global Forum on Information Systems and Network Security held on 13 and 14 October 2003 in Oslo (Norway) took stock of the first year of application of the OECD guidelines published in 2002.

In November 2003, OECD published a report containing guidelines on the protection of privacy and best practices, which brought together all of the work thus far carried out with a view to ensuring an effective policy for protecting the private user online.

For e-commerce to be trustworthy, infrastructure and services must be reliable, transactions secure and private, and personal data protected. The OECD Working Party on Information Security and Privacy promotes a global, coordinated approach to policymaking in these areas to help build trust online. The report provides a set of regulatory and self-regulatory approaches, including legal, technical and educational solutions according to the cultural and social context of the environment. It draws attention to the need for close cooperation among all players within the sector, and is organized as follows:

Part I

Overview of the work done by the OECD Working Party on Information Security and Privacy.

Part II

Guidelines based on the work described in Part I.

Part III

This part of the document includes all of the documents presented in Part I, and specifically:

- Guidelines on the protection of privacy and transborder flows of personal data.
- Ministerial declaration on the protection of privacy on global networks.

Inventory of instruments and mechanisms contributing to the implementation and enforcement of the OECD privacy guidelines on global networks. This document is to be found at:
http://www.oecd.org/dataoecd/12/54/2092454.pdf

On 1 December 2003, OECD set up a new "Culture of security" website dedicated to combating attacks against information network and system security. The address of this site is:
http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase

NOTES

1 – All of the aforementioned OECD documents may be accessed via the URL:

http://www.oecd.org/document/20/0,2340,en_2649_33703_15589524_1_1_1_1,00.html

2 – The 26th International Conference on Privacy and Personal Data Protection will be held from 14 to 16 September 2004 in Warsaw (Poland).

3 – An anti-spam group was created on 22 October 2004, bringing together the 30 OECD member states, the private sector, civil society and international organizations, including ITU. Its work is scheduled to last two years.

5.2 Council of Europe

The Council of Europe decided to take up the challenge, taking into account the need to safeguard human rights in the new information society and establishing principles for international cooperation through relevant international instruments in criminal matters and arrangements agreed on the basis of uniform or reciprocal legislation, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. This exploration of the issue by the Council of Europe resulted in the signature of a multinational convention on cybercrime.

Convention on cybercrime (Council of Europe)

In November 1996, the European Committee on Crime Problems decided to set up a committee of experts. Drawing on the experts' work, a convention on cybercrime was drafted and presented for signature on 23 November 2001 at the International Conference on Cybercrime in Budapest. That international convention was signed by most European countries, including most of the countries of Central and Eastern Europe that are candidates for future European Union membership, as well as many other countries around the world (the United States, Japan, South Africa, Canada).

The key aims of the convention are:

1) to harmonize domestic criminal law provisions and related provisions pertaining to cybercrime;
2) to provide domestic criminal procedural law with the necessary powers to investigate and prosecute cybercrime offences, as well as other offences committed by means of a computer system or offences in respect of which evidence exists in electronic form;
3) to implement a rapid and effective international cooperation mechanism.

The main subject areas covered by the convention are as follows:

- offences against the confidentiality, integrity and availability of computer data and systems:
  - illegal access
  - illegal interception
  - data interference and system interference

  - misuse of devices
- computer-related offences:
  - computer-related forgery
  - computer-related fraud
- content-related offences
- offences related to infringements of copyright and related rights
- ancillary liability and sanctions:
  - attempt and aiding or abetting
  - corporate liability
  - sanctions and measures.

The convention also includes chapters on:

- procedural law (criminal law, procedural law and jurisdiction)
- international cooperation:
  - general principles relating to international cooperation, extradition and mutual assistance requests in the absence of applicable international agreements
  - specific provisions.

The Council of Europe has taken account of the fact that globalization poses risks which may lead to exclusion and increased inequality, often based on race or ethnicity. Thus, even though advances in the spheres of technology, economics and trade may bring the world's peoples closer together, racial discrimination, xenophobia and other forms of intolerance continue to exist in our societies.

Accordingly, on 7 November 2002 the Council of Europe adopted an Additional Protocol to the Convention on cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.

The full text of the two documents referred to above is accessible at the webpages <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm>and <http://conventions.coe.int/Treaty/EN/Reports/Html/189.htm>.

5.3 European Union

The Council of the European Union (EU) at its June 2000 session in Lisbon adopted the eEurope 2002 Action Plan: essentially, universal internet connectivity as a means to stimulate significant economic growth among the member countries.

The principal results obtained by putting eEurope 2002 into practice have been as follows:

- number of households with internet connections has doubled
- Telecoms European working framework in place
- cost of internet access has dropped (http://europa.eu.int/eeurope).

The Barcelona European Council asked the EU to build on the results of eEurope 2002 to put in place eEurope 2005. The Action Plan would have four priorities:

- modernize online public services: e-government, e-learning and e-health
- dynamic e-business environment
- broadband access at competitive prices
- secure information infrastructure.

For information security, the EU is following a strategy based on the security of communication networks [Network Information Society COM/2001 398 of 6 June 2001], the subject of a Resolution of 28 January 2002 (http://register.consillium.eu.int/pdf/en/01/st15/1512enI.pdf), and more recently the Commission proposed a decision for a general framework on attacks against information systems (http://europa.eu.int/comm/dgs/justice-home/index-en.htm), COM(2002) 173 final of 19 April 2002.

The proposed actions are listed below.

- **Cybersecurity task force (CSTF).** By end-2003, the CSTF was to have been operational. Based on proposals from the European Commission, Council and Parliament should adopt a legal base as quickly as possible, taking into account the interlinked dimension of network and information security. The CSTF should become a centre of competence on security questions, and Member States should develop a concept for a European computer attack alert system together with the European Commission.
- **Culture of security.** By end-2005, a "culture of security" in the design and implementation of information and communication products should be achieved (intermediate report end-2003).
- **Secure communications between various public services.** By end-2003, the Commission and Member States will examine the possibilities to establish a secure communications environment for the exchange of classified government information.

eEurope 2005

The European Council at Barcelona in 2002 invited the Commission to establish an eEurope action plan aimed at "the widespread availability and use of broadband networks throughout the Union by 2005 and the development of internet protocol IPv6 …. and the **security of networks and information** …. and eBusiness".

Section 3.1.3 of the EU document entitled "eEurope 2005: An information society for all" concerns a secure information infrastructure.

The European Union has already launched a comprehensive strategy based on the Communications on network security[1], cybercrime[2], and the current[3] and forthcoming data protection directive regarding electronic communications. The suggested approach was endorsed and further developed by the Council Resolution of 28 January 2002[4] and by the recent Commission proposal for a Council Framework Decision on attacks against information systems[5].

Community research activity on security will continue under the Sixth Framework Programme. Priorities will be: trustworthy network and information infrastructures with an emphasis on emerging technologies (e.g. broadband, wireless architectures, ambient intelligence); the identification of vulnerabilities and inter-dependencies in infrastructures. It also intends to support standardization with a view to wider use of open standards and open source software. Research activities should also take into account the "human factor" in security, e.g. basic security standards, user-friendliness of systems.

---

1 Network and Information Security: Proposal for a European Policy Approach, COM(2001) 298 of 6.6.20

2 Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 of 22.1.2001.

3 Directive 97/66/EC of the European Parliament and of the Council on 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24 of 30.1.1998.

4 http://register.consilium.eu.int/pdf/en/01/st15/15152en1.pdf

5 http://europa.eu.int/comm/dgs/justice_home/index_en.htm COM(2002) 173 final of 19.4.2002.

The following actions are proposed to meet these objectives:

1) Cybersecurity task force

   Council and Parliament will be able to adopt the necessary legal base as quickly as possible, taking into account the cross-pillar dimension of network and information security. Member States and the private sector should support the activities of CSTF. It should become a centre of competence on security questions, e.g. to develop with Member States a concept for a European computer attack alert system; to facilitate cross-pillar discussion; and to improve transborder cooperation.

2) Culture of security

   By end-2005, a "culture of security" in the design and implementation of information and communication products should be achieved. The private sector should develop good practices and standards and promote their consistent application. The Commission intends to support projects and will work to raise awareness of security risks in all users. An intermediate report of progress will be issued end 2003 and a final assessment by end 2005.

3) Secure communications between public services

   By end-2003, the Commission and Member States will examine the possibilities to establish a secure communications environment for the exchange of classified government information.

NOTE – In 2004 the European Commission set up the European Network and Information Security Agency (ENISA). This is a centre of excellence focussing dialogue between the public and private sectors with a view to elaborating guidelines and best practices on security within the EU.

5.4 National Strategy to Secure Cyberspace (USA)

After studies wanted by the White House concerning the protection against the debilitating disruption of the operation of information systems and the protection of the people, economy and national security of the United States; reports were published in February 2003.

This National Strategy to Secure Cyberspace is part of the overall effort to protect the American Nation. It is an implementing component of the National Strategy for Homeland Security and is complemented by a National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector, and the American people.

- Strategic Objectives

  Consistent with the National Strategy for Homeland Security (25 November 2002, Department of Homeland Security – DHS – has created) the strategic objectives of the National Strategy to Secure Cyberspace are to:

  – prevent cyber attacks against America's critical infrastructures;

  – reduce national vulnerability to cyber attacks; and

  – minimize damage and recovery time from cyber attacks that do occur.

After a chapter about cyberspace threats and vulnerabilities, it is given "National Policy and Guiding Principles". The protection of the cyber systems is essential to every sector of the economy, the development and implementation of the federal program directive decided in October 2001 has been guided by the following principles:

1) National Effort;

2) Protect Privacy and Civil Liberties;

3) Regulation and Market Forces;

4) Accountability and Responsibilities;

5) Ensure Flexibility;

6) Multi-Year Planning.

Critical Priorities for Cyberspace Security

The National Strategy to Secure Cyberspace articulates five national priorities including:

I. A National Cyberspace Security Response System;

II. A National Cyberspace Security Threat and Vulnerability Reduction Program;

III. A National Cyberspace Security Awareness and Training Program;

IV. Securing Governments' Cyberspace; and

V. National Security and International Cyberspace Security Cooperation.

The first priority focuses on improving our response to cyber incidents and reducing the potential damage from such events. The second, third, and fourth priorities aim to reduce threats from, and our vulnerabilities to, cyber attacks. The fifth priority is to prevent cyber attacks that could impact national security assets and to improve the international management of and response to such attacks.

For each national priority, **Actions and Recommendations (A/R)** are given, the Appendix of the report includes a resume of these A/R.

5.5 Security measures taken by software writers

Software writers have released some of their source code to increase security, in response to demands from governments and public organizations for more transparency.

a) Following Windows in 2001, Microsoft decided in September 2004 to allow core consultation of its Office 2003 programs (Word for word processing, Excel for spreadsheets and Outlook for e-mail). In this way, public and government organizations will have a better understanding of the manner in which files are stored and carry on dialogue and exchanges with Microsoft engineers in parallel: *administrations are obliged to comply with legal obligations for long-term storage.*

In September 2004:

- Some thirty countries, including China, Australia and Spain, have already signed an agreement for Windows; meanwhile, the United Kingdom is the first country to sign an access agreement for Office source.

- In France, some thirty organizations (mostly university-affiliated) have signed an agreement with Microsoft under the programme for the distribution of Windows and Office source code.

b) Software writers have begun providing free unhindered access to their source code right from the time their products come on the market; the Linux operating system, for example, and other software manufacturers in areas such as application servers, portals or office software.

6 ISO Standards

Since 1996, ISO/IEC 15408 has been used to conduct certification for information system security measures. It is better known under the name of "common criteria". It is the result of a progressive convergence between TCSEC (Trusted Computer Systems Evaluation Criteria, also known as the "Orange Book") and ITSEC (Information Technology Security Evaluation Criteria), both of which were developed by merging different national criteria.

In December 2000 a British standard, BS 7799-1, was adopted by the International Organization for Standardization (ISO) and given the reference ISO/IEC 17799.

ISO/IEC 17799 observes that, in general, information systems have not been designed to be secure. Technical protection measures accordingly have a limited impact, and must be complemented by an appropriate organization and procedures.

The standard therefore proposes a body of guidelines and directions describing the best practices for information security, in the broadest sense. The outlook should not be restricted to IT systems only; rather, the aim is to take into account information in all its forms, information being the organization's chief asset.

The rules are broken down into ten "clauses":

1) **Security policy**. This clause describes a document outlining the organization's security policy in terms of responsibilities, approval, review and changes.

2) **Organizational security**. The guidelines under this clause deal with the role of the various players involved in security policy, in particular the committee responsible for the organization's strategy in this domain. The committee is set up by the senior executive and acts to define and oversee security policy, The key person in this organization is the information system security officer (ISSO). This clause also examines some contractual aspects of protecting third-party access to the information system.

3) **Asset classification and control**. The objective is to maintain an appropriate level of protection for all information system assets by compiling an inventory of assets, classifying them and identifying owners who will be responsible for them.

4) **Personnel security**. The rules that come under this clause are intended to minimize the risk of human error, theft, fraud or misuse of IT resources, by informing users about the risks and dangers to which their information may be exposed.

5) **Physical and environmental security**. The objective is to prevent unauthorized access, damage to and interference with information, on the premises of the organization.

6) **Operations and networks**. The objective is to minimize the risks and impact of breakdowns through correct and secure operation of information processing facilities, by ensuring the integrity and availability of information, processing and communications.

7) **Access control**. The rules under this clause are aimed at managing and controlling online access to information, through the protection of systems in networks and the detection of unauthorized activities.

8) **System development and maintenance**. This section is based on the principle that security should be included right from the requirements phase; it offers guidelines for preventing loss, modification or misuse of information in operating systems and application software.

9) **Continuity management**. This clause is intended to improve the organization's ability to respond rapidly to interruptions of critical processes caused by failures, accidents, and other emergencies and disasters.

10) **Compliance**. Compliance concerns statutory and regulatory requirements, the effectiveness of the procedures that have been adopted, with respect to security policy, to meet the objectives set forth by the organization's management; and the effectiveness of the traceability and compliance arrangements that have been put in place, in particular activity records, audits and transaction logs.

While ISO/IEC 17799 has given great prominence to BS 7799-1, which it largely reproduces, the second part of this standard, BS 7799-2, has not yet been proposed to ISO and is not as well known. Nonetheless, this is a particularly important document which must be understood if one wishes to grasp the overall mechanism by which an organization defines its own strategy for managing information security. In its latest version, dating from September 2002, BS 7799-2 proposes harmonization with ISO 9001:2000 (quality management and assurance) and ISO 14001 (environmental management), and with the OECD guidelines (see section 5.1). It is thus a genuine certification reference that is already in broad use internationally, in Great Britain, Australia, Norway, Brazil and Japan, for example.

7 World Summit on the Information Society

The first phase of the World Summit on the Information Society (WSIS), organized by ITU under the auspices of the United Nations, was held in Geneva from 10 to 12 December 2003. It involved heads of states and governments, secretaries-general of the specialized agencies of the United Nations, private-sector representatives and representatives from the media and from civil society so as to coordinate the global advent of the information society in a smooth manner. During the first phase, a working document was examined that related to a list of subjects from an established framework. The subjects are listed below:

1) Information and communication infrastructure: funding and investment, affordability, development and sustainability.

2) Access to information and knowledge.

3) Role of countries, of the private sector and of civil society in promoting ICTs in the service of development.

4) Capacity building: human resource development, education and training.

5) Security.

6) Enabling environment.

7) Promotion of object-oriented applications: development of ICTs for all, e.g. e-government, e-commerce, e-learning and e-health.

8) Cultural and linguistic diversity and content, media development.

9) How to overcome the obstacles that stand in the way of the creation of a people-centred Information Society.

WSIS resulted in the adoption, on 12 December 2003, of a **Declaration of Principles** and an **Action Plan**.

Those passages in the two adopted documents that relate to cybersecurity are listed below.

7.1 Declaration of Principles

Building the Information Society: a global challenge in the new Millennium

A Our common vision of the information society

We, the representatives of the peoples of the world, assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to

build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.

B An information society for all: key principles

5 Building confidence and security in the use of ICTs

35. Strengthening the trust framework including network and information security authentication, privacy and consumer protection is a prerequisite to developing the information society and building confidence among users of ICTs. A global culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cybersecurity, it is important to enhance security and to ensure the protection of data and privacy, [as well as to avoid the creation of barriers to access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

36. While recognizing the principles of universal and non-discriminatory access to ICTs for all nations, we support the activities conducted by the United Nations to prevent the potential use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security, and threaten to adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes while respecting human rights.

37. Spam is a significant and growing problem for users, networks and the internet as a whole. Spam and cybersecurity should be dealt with at appropriate national and international levels.

48. The internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the internet, taking into account multilingualism.

7 ICT applications: benefits in all aspects of life

51.h Develop a framework for the secure storage and archival of documents and other electronic records of information.

51.i Governments and stakeholders should actively promote user education and awareness about online privacy and the means of protecting privacy.

Invite stakeholders to ensure that practices designed to facilitate electronic commerce also permit consumers to have a choice over whether or not to use electronic communication.

C7 ICT applications: benefits in all aspects of life

15 E-government

a) Implement e-government strategies focusing on applications aimed at innovating and promoting transparency in public administrations and democratic processes, improving efficiency and strengthening relations with citizens.

b) Develop national e-government initiatives and services, at all levels, adapted to the needs of citizens and business, to achieve a more efficient allocation of resources and public goods.

10 Ethical dimensions of the Information Society

58. The use of ICTs and content creation should respect human rights and fundamental freedoms of others, including personal privacy, and the right to freedom of thought, conscience, and religion in conformity with relevant international instruments.

64. The core competences of ITU in the fields of ICTs – assistance in bridging the digital divide, international and regional cooperation, radio spectrum management, standards development and the dissemination of information – are of crucial importance for building the Information Society.

7.2 Action Plan

A Introduction

2) The Information Society is an evolving concept that has reached different levels across the world, reflecting the different stages of development. Technological and other change is rapidly transforming the environment in which the Information Society is developed. The Plan of Action is thus an evolving platform to promote the Information Society at the national, regional and international levels. The unique two-phase structure of the WSIS provides an opportunity to take this evolution into account.

B Objectives, goals and targets

5) Specific targets for the Information Society will be established as appropriate, at the national level in the framework of national e-strategies and in accordance with national development policies, taking into account the different national circumstances. Such targets can serve as useful benchmarks for actions and for the evaluation of the progress made towards the attainment of the overall objectives of the Information Society.

C Action Lines

C1 The role of governments and all stakeholders in the promotion of ICTs for development

8.1 The effective participation of governments and all stakeholders is vital in developing the Information Society requiring cooperation and partnerships among all of them.

a) Development of national e-strategies, including the necessary human capacity building, should be encouraged by all countries by 2005, taking into account different national circumstances.

C5 Building confidence and security in the use of ICTs

12 Confidence and security are among the main pillars of the Information Society

a) Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate fora to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.

b) Governments, in cooperation with the private sector, should prevent, detect and respond to cybercrime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.

c) Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy.

d) Take appropriate action on spam at national and international levels.

e) Encourage the domestic assessment of national law with a view to overcoming any obstacles to the effective use of electronic documents and transactions including electronic means of authentication.

f) Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection.

g) Share good practices in the field of information security and information network security and encourage their use by all parties concerned.

h) Invite interested countries to set up focal points for real-time incident handling and response, and develop a cooperative network between these focal points for sharing information and technologies on incident response.

i) Encourage further development of secure and reliable applications to facilitate online transactions.

j) Encourage interested countries to contribute actively to the ongoing United Nations activities to build confidence and security in the use of ICTs.

C6 Enabling environment

13) To maximize the social, economic and environmental benefits of the Information Society, governments need to create a trustworthy, transparent and non-discriminatory legal, regulatory and policy environment. Actions include:

e) Governments should continue to update their domestic consumer protection laws to respond to the new requirements of the Information Society.

c) Support international cooperation initiatives in the field of e-government, in order to enhance transparency, accountability and efficiency at all levels of government.

C11 International and regional cooperation

26) International cooperation among all stakeholders is vital in implementation of this plan of action and needs to be strengthened with a view to promoting universal access and bridging the digital divide, inter alia, by provision of means of implementation.

D Digital Solidarity Agenda

27) The Digital Solidarity Agenda aims at putting in place the conditions for mobilizing human, financial and technological resources for inclusion of all men and women in the emerging Information Society. Close national, regional and international cooperation among all stakeholders in the implementation of this Agenda is vital.

E Follow-up and evaluation

28) A realistic international performance evaluation and benchmarking (both qualitative and quantitative), through comparable statistical indicators and research results, should be developed to follow up the implementation of the objectives, goals and targets in the Plan of Action, taking into account different national circumstances.

e) Develop and launch a website on best practices and success stories, based on a compilation of contributions from all stakeholders, in a concise, accessible and compelling format, following the internationally-recognized web accessibility standards. The website could be periodically updated and turned into a permanent experience-sharing exercise.

Tunis 2005: the second phase

The second phase of the World Summit, which will be hosted by the government of Tunisia, will take place from 16 to 18 November 2005 at Tunis. It will be devoted in the main to development-related issues, and it will measure the progress made and adopt another action plan, if this is considered necessary.

In conclusion, among the goals of WSIS the following may be noted:

Build confidence and security in ICT utilization

•Authentication • Confidence and security building • Consumer protection • Fighting ICT abuse • Fighting spam • Cybercrime • Cybersecurity • Data protection • Information security and network security • Network integrity • Security of on-line transactions • Privacy protection • Real-time incident handling • Secure, reliable applications.

NOTE – For more information, see the website at www.itu.int/wsis or www.un.org/milleniumgoals/, the United Nations site which gives the Millennium development goals, which can be correlated with those of the Geneva phase of WSIS.

8 Activities under way within ITU

8.1 WTSA-04 Resolutions (security)

The World Telecommunication Standardization Assembly held in Brazil 5-14 October 2004 adopted and approved a number of new resolutions concerning security. They are the first of their kind to be adopted by a high-level ITU assembly following Resolution 130 of the Plenipotentiary Conference (Marrakesh, 2002):

- **Resolution 50: Cybersecurity**

Resolution 50 opens with a preamble recognizing "the vigorous activity and interest in the development of security standards and Recommendations" within ITU, particularly in SG 17, and goes on to record that the Assembly resolved as follows:

1 that ITU-T evaluate existing and evolving new Recommendations, and especially signalling and communications protocol Recommendations, with respect to their robustness of design and potential for exploitation by malicious parties to interfere destructively with their deployment in the global information and communication infrastructure;

2 that ITU-T continue to raise awareness, within its area of operation and influence, of the need to defend information and communication systems against the threat of cyber attack, and continue to promote cooperation among appropriate entities in order to enhance exchange of technical information in the field of information and communication network security[.]

The Assembly went on to instruct the Director of the Telecommunication Standardization Bureau

to develop, in consultation with the chairman of [the Telecommunications Standardization Advisory Group] and the appropriate study group chairmen, a plan to undertake the abovementioned evaluation of relevant Recommendations at the earliest possible time considering resources available and other priorities, and to provide updates of the progress regularly to TSAG,

and

1 to include in the annual report to the Council specified in Resolution 130 (Marrakesh, 2002) of the Plenipotentiary Conference the progress in the evaluations under resolves above;

2 to continue to take appropriate action to publicize the need to defend information and communication networks against the threat of cyber attack, and to cooperate with other relevant entities in these efforts;

3 to liaise with other bodies active in this field, such as the International Organization for Standardization (ISO) and the Internet Engineering Task Force (IETF),

Finally, the Assembly invited Member States, Sector Members and Associates to "participate actively in the implementation of this resolution and the associated actions".

- **Resolution 51: Combating spam**

Resolution 51 opens with a preamble in which the World Telecommunication Standardization Assembly (Florianópolis, 2004) recognizes the relevant findings of the World Summit on the Information Society, and then goes on as follows:

[C]onsidering

a) relevant provisions of the basic instruments of ITU;

b) that agreed measures to combat spam fall within Goal 4 of the strategic plan for the Union for [2002]-2007 (Part I, clause 3) set out in Resolution 71 (Rev.Marrakesh, 2002) of the Plenipotentiary Conference;

c) Resolution 52 on countering spam by technical means;

d) the report of the chairman of the ITU WSIS thematic meeting on countering spam, which advocated a comprehensive approach to combating spam, namely:

   i) strong legislation,

   ii) the development of technical measures,

iii) the establishment of industry partnerships,

iv) education, and

v) international cooperation,

instructs the Director of the Telecommunication Standardization Bureau, in cooperation with the Directors of the other Bureaux and the Secretary-General

to prepare urgently a report to the Council on relevant ITU and other international initiatives for countering spam, and to propose possible follow-up actions for consideration by the Council,

invites Member States

to contribute to this work,

further invites Member States

to take appropriate steps within their national legal frameworks to ensure that appropriate and effective measures are taken to combat spam.

- **Resolution 52: Countering spam by technical means**

Resolution 52 opens with a *considering* section (*a* to *f*) and then goes on as follows:

[R]ecognizing

a) relevant provisions of the basic instruments of ITU;

b) that spam creates telecommunication network security problems, including by being a vehicle for spreading viruses, worms, etc.;

c) that spam is a global problem that requires international cooperation in order to find solutions;

d) that [solving] the issue of spam is a matter of urgency,

instructs the relevant study groups

in cooperation with the Internet Engineering Task Force (IETF) and other relevant groups, to develop, as a matter of urgency, technical Recommendations, including required definitions, on countering spam, as appropriate, and to report regularly to [TSAG] on their progress,

instructs the Director of [TSB]

to provide all necessary assistance with a view to expediting such efforts, and to report on this to the Council.

In conclusion, it is SG 17 (see § 8.2.2) which will be principally responsible for applying these three Resolutions. In addition, a report from the Director of TSB, concerning the application of these three Resolutions, is to be submitted to WTSA-08.

NOTE – The documents cited above are accessible on the ITU-T website for WTSA-04.

8.2 ITU-T study groups

8.2.1 2001-2004 study period

This section describes work being done in ITU-T study groups on the subject of information and communication network security.

- ITU-T Study Group 2 is currently working on draft Recommendations dealing with security requirements for telecommunication networks (E.408), the organization of incident management activities and the handling of incidents involving security (E.409 – submitted for approval on 18 May 2004 (Working Party 2/2)).

- ITU-T Study Group 4 has prepared a series of Recommendations dealing with security aspects of telecommunication management networks (TMNs): M.3010, "Principles for a telecommunication management network"; M.3210.1, "TMN management services for IMT-2000 security management"; M.3013, "Considerations for a telecommunication management network"; M.3016, "Overview of TMN security"; M.3210, "TMN management services for IMT-2000 security management"; M.3320, "Management requirements framework for the TMN X interface"; M.3400, "TMN management functions"; Q.813, "Security transformations application service element for remote operations service element (STASE-ROSE)"; Q.815, "Specification of a security module for whole message protection"; Q.817, "TMN PKI – Digital certificates and certificate revocation lists profiles". Work on security issues is currently under way in connection with Questions 7, 9, 10 and 18/4.

- ITU-T Study Group 9 has prepared Recommendation J.170, "IPCablecom security specification", in the framework of its IPCablecom project. This Recommendation deals with authentication, access control, message and bearer content integrity, confidentiality and non-repudiation security services.

- ITU-T Study Group 11 is currently developing network control and signalling protocols, integrating security needs identified by the competent Study Groups and other bodies. Related studies are being carried out by Working Party 1/11 (Questions 1/11, 2/11, 3/11, 4/11 and 5/11), Working Party 2/11 (Question 6/11) and Working Party 3/11 (Question 11/11).

- ITU-T Study Group 13 is examining the security aspects of multi-protocol and IP-based networks. This area falls within ITU-T's NGN 2004 and IP projects. At the last meeting of Study Group 13 (29 October to 8 November 2002), it was decided that a clause on security would henceforth be added to all future texts, including those currently in preparation. Recommendation Y.110 discusses certain general aspects of security with respect to the world information infrastructure. As part of the consideration of Question 1/13, a new Recommendation Y.1271 is being formulated regarding network requirements and capabilities to support emergency communications. A new Recommendation Y.140.1, which is also being prepared as part of the consideration of Question 1/13, is of particular interest as it deals with a number of security attributes at possible interconnection points between network operators and service providers. Recommendation Y.140, "Global Information Infrastructure (GII) – Reference points for interconnection framework" provides general information having enabled the preparation of Recommendation Y.140.1.

- The contribution by ITU-T Study Group 15 to security standardization activities is concerned with two areas: the reliability and security of communications.

- Question 9/15, "Transport equipment and network protection/restoration", deals with SDH protection switching (Recommendation G.841, "Types and characteristics of SDH network protection architectures", and Recommendation G.842, "Interworking of SDH network protection architecture") and OTN protection switching (draft Recommendations G.808.1 and G.808.2, "Generic protection switching", draft Recommendations G.873.1 and G.873.2, "OTN protection"). Specifications in regard to network restoration are to be added to the Recommendations on equipment and network restoration.

- Question 15/15, “Characteristics and test methods of optical fibres and cables”, Question 16/15, “Characteristics of optical systems for terrestrial transport networks”, Question 17/15, “Characteristics of optical components and subsystems”, and Question 18/15, “Characteristics of optical fibre submarine cable systems”, all contain some element concerned with reliability. Recommendation G.911, “Parameters and calculation methodologies for reliability and availability of fibre optic systems”, is also concerned with this subject. As well, Questions 15/15, 16/15, 17/15 and 18/15 are concerned with studying the reliability and availability of cables and optical fibres, and of terrestrial and submarine components, subsystems and optical systems.

  All the work concerned with the security of communications falls under Question 14/15, “Network management for transport systems and equipment”. Recommendations G.784, “synchronous digital hierarchy (SDH) management” and G.874, “Management aspect of the optical transport network element”, deal with fault, configuration, accounting, performance and security management (FCAPS) for SDH and OTN network elements. In these Recommendations, security management aspects are to be covered by an adjunct study. Recommendation G.7712/Y.1703, “Architecture and specification of data communication network” deals with security aspects of Management Communication Networks (MCNs) and Signalling Communication Networks (SCNs).

- Within the framework of Question G.16

  (http://www.itu.int/ITU-T/studygroups/com16/sg16-qg.html), ITU-T Study Group 16 has developed and is further revising a number of Recommendations to assure the security of various protocol families and audiovisual conferencing systems, such as Recommendations H.320 on ISDN, H.310 on broadband ISDN, H.324 on PSTN and third-generation mobile networks, and H.323 on packet based networks (including IP telephony). Recommendations H.233, “Confidentiality system for audiovisual services”, and H.234, “Encryption key management and authentication system for audiovisual services” (for H.320 systems) are currently in force. The H.SETS “Security for emergency telecommunication systems” series of Recommendations are currently in preparation, and version 3 of Recommendation H.235, “Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals” has recently been approved. Question I/16 has recently been approved, calling for studies on assuring security for emergency and disaster relief operations (e.g. preventing the theft of services, authorizing users, assuring confidentiality) with the aid of multimedia communications, in conjunction with Question G.16, “Security of multimedia systems and services”, and in collaboration with other Study Groups and other standards bodies.

- ITU T Study Group 17 has been designated the Lead Study Group for Telecommunication Security. Within Study Group 17, this effort is coordinated by Q.4/17, Communications Systems Security Project. Information pertaining to this effort can be accessed through the Study Group 17 webpage at the ITU website (http://www.itu.int/ITU-T/studygroups/com17/tel-security.html).

- Study Group 17 has prepared a catalogue of ITU Recommendations concerned with communication system security, and a compendium of security definitions drawn from approved ITU-T Recommendations. Both the catalogue of Recommendations and the compendium of definitions can be accessed through the Study Group 17 webpage at the ITU website (http://www.itu.int/ITU-T/studygroups/com17/cssecurity.html). Study Group 17 has also drawn up a compendium of security definitions approved by ITU-T; this document, together with its addendum, allows for an overall understanding of the security terms used by the various ITU-T working parties and study groups (see § 8.7). The working party responsible for Question 10/17, “Security requirements, models and guidelines for communication systems and services”, regularly updates its lists of communication system security information and has developed a series of new Recommendations.

Study Group 17 has a number of Questions pertaining to Security. They are:

– Q.2/17, Directory Services, Directory Systems, and Public-key/Attribute Certificates. Under this Question, the well-known Recommendation X.509, "Public-key and attribute certificate framework", is the basis of public key infrastructures (PKIs) and privilege management infrastructures (PMIs), and an updated edition is expected to be approved in 2005.

– Q.4/17, Communications Systems Security Project. This Question is responsible for the overall vision and coordination of security work.

– Q.5/17, Security Architecture and Framework. A substantial set of Recommendations on security is contained in the X.800 series. In 2003, an important addition was added – Recommendation X.805 covering Security architecture for systems providing end-to-end communications.

– Q.6/17, Cybersecurity. Studies have begun on addressing many issues concerned with security in cyberspace.

– Q.7/17, Security Management. Recommendation X.1051 on Information security management system – Requirements for telecommunications (ISMS-T) was approved in 2004.

– Q.8/17, Telebiometrics. Recommendation X.1081 on The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics was approved in 2005. Additional information is provided in section 8.4.

– Q.9/17, Secure Communication Services. Two Recommendations on mobile security were approved in 2004. They are X.1121 on Framework of security technologies for mobile end-to-end communications and X.1122 on Guideline for implementing secure mobile systems based on PKI.

ITU-T's standardization activities will be carried out under a new ITU-T project on security, which was approved at the meeting of Study Group 17 held in November 2002.

Furthermore, in order to accommodate the increase in security-related activities, Study Group 17 decided in March 2004 to divide Question 10/17 into six new Questions, from G to L/17 for the study period 2005-2008.

NOTE – The Special Study Group "IMT-2000 and beyond" has included security as one of the key points in its basic Recommendations for members of the IMT-2000 (3G) family. The subjects covered include, *inter alia*: evaluation of perceived threats and list of security requirements to deal with them; security principles and objectives; a well-defined security architecture (i.e. security mechanisms and characteristics); needs in regard to cryptographic algorithms; conditions for lawful interception, and lawful interception functions and architectures. These studies are being carried out under Question 3/SSG.

8.2.2 2005-2008 period

Pursuant to **Resolution 2 of WTSA-04**, the following Study Groups were established for the 2005-2008 period:

SG 2 **Operational aspects of service provision, networks and performance** – Lead study group for service definition, numbering and routing

SG 3 **Tariff and accounting principles including related telecommunication economic and policy issues** – Study group for tariff and accounting principles and for telecommunication economic and policy matters

SG 4 **Telecommunication management** – Lead study group on telecommunication management

SG 5 **Protection against electromagnetic environment effects** – Study group for protection against electromagnetic environment effects

SG 6 **Outside plant and related indoor installations** – Study group for outside plant and related indoor installations – this could be shown as being in addition to the LS4 function

SG 9 **Integrated broadband cable networks and television and sound transmission** – Lead study group on integrated broadband cable and television networks

SG 11 **Signalling requirements and protocols –** Lead study group on signalling and protocols. Lead study group on intelligent networks

SG 12 **Performance and quality of service –** Lead study group on quality of service and performance

SG 13 **Next-generation networks –** Lead study group for NGN and satellite matters

SG 15 **Optical and other transport network infrastructures –** Lead study group on access network transport – Lead study group and on optical technology

SG 16 **Multimedia terminals, systems and applications –** Lead study group on multimedia terminals, systems and applications – Lead study group on ubiquitous applications (”e-everything”, such as e-health and e-business)

SG 17 **Security, languages and telecommunication software –** Lead study group on telecommunication security. Lead study group on languages and description techniques

SG 19 **Mobile telecommunication networks –** Lead study group on mobile telecommunication networks and for mobility

Among the changes to the allocation of work within the ITU-T study groups, the following should be noted:

Study Group 2 including the internet, as it is supposed to “recommend traffic engineering planning and dimensioning guidance for the implementation and operation of all types of networks and network elements”.

Study Group 11

Study Group 11 is to develop Recommendations on the fundamental aspects of network signalling and control architecture and protocols for networks, including convergence toward NGN, in cooperation and close coordination with other study groups responsible for Questions dealing with other networks and NGN.

Recommendations are to be developed on the following Questions considering convergence of fixed and mobile networks:

- network signalling and control functional architectures in emerging NGN environments;
- application control and signalling requirements and protocols;
- session control and signalling requirements and protocols;
- bearer control and signalling requirements and protocols;
- resource control and signalling requirements and protocols;
- signalling and control requirements and protocols to support attachment in NGN environments.

Study Group 11 is to lend assistance in the preparation of a handbook on the deployment of packet-based networks.

Study Group 11 is to reuse, where appropriate, protocols that are being developed by other SDOs, in order to maximize standards investments.

Study Group 11 is to work on enhancements to existing Recommendations on access and internetwork signalling protocols of BICC, ATM, N-ISDN and PSTN, i.e., SS No. 7, DSS1 and DSS2, etc. The objective is to satisfy business needs of member organizations that wish to offer new features and services on top of networks based on existing Recommendations.

Study Group 11 is encouraged to hold collocated meetings of relevant activities with those of Study Group 13 and Study Group 19 whenever possible, as determined by the study group management teams.

Study Group 17

Study Group 17 is responsible for studies relating to security, the application of open system communications including networking and directory, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems.

In the area of security, Study Group 17 is responsible for developing the core Recommendations on security such as security architecture and frameworks. In addition, Study Group 17 provides overall coordination of security work in the ITU-T.

In the area of open system communication, Study Group 17 is responsible for Recommendations in the following areas:

- open systems interconnection (OSI) (X.200-, X.400-, X.600-, X.800-series, etc.);
- directory services and systems (F.500- and X.500-series); and
- open distributed processing (ODP) (X.900-series).

In the area of languages, Study Group 17 is responsible for studies on modelling, specification and description techniques. This work, which includes languages such as ASN.1, SDL, MSC, eODL, URN, and TTCN, will be developed in line with the requirements of and in cooperation with the relevant study groups such as SG 4, SG 9, SG 11, SG 13, SG 15 and SG 16.

In the area of software aspects of telecommunication systems, this work will concentrate on aspects for which the industry deems it useful to apply ITU-T Recommendations in order to enhance the use of software technology with associated processes and in order to stimulate the market place for such technology.

The work of Study Group 17 will be coordinated with developments carried out by other standardization bodies such as ISO/IEC JTC1, IETF and ETSI. Applicable work done in forums and consortia, such as OMG, TMF, SDL Forum Society, ASN.1 Consortium, OASIS, etc., will also be considered in order to get the maximum synergy and to minimize the efforts in the development of new Recommendations.

Study Group 19

Study Group 19 has the primary responsibility within ITU-T for overall network aspects of mobility and mobile communication networks, including IMT-2000 and beyond IMT-2000. It is responsible for:

- service and network capability requirements and network architecture;
- mobility management;

- identification of existing and evolving IMT-2000 systems;
- preparation of a handbook on IMT-2000;
- convergence of evolving IMT-2000 networks with evolving fixed networks;
- providing a migration path regarding network aspects and mobility from existing IMT-2000 systems towards systems beyond IMT-2000;
- enhancing an overview road map on network aspects and mobility of existing IMT-2000 systems specified by ITU-T and external organizations (e.g. SDOs, partnership projects (PPs), IETF, relevant external forums, etc.); and
- studying mobility management requirements and techniques with the aim of allowing for global mobility between evolving IMT-2000 systems and systems beyond IMT-2000 specified by external organizations.

The points above include the development of a long-term common IP-based network architecture applicable to mobile communication networks, including mobility within next-generation networks. Additionally, considering the ongoing evolutionary directions of network infrastructure, they include near-term IP-based internetworking.

In addition, Study Group 19 will study:

- harmonization of different IMT-2000 family member standards as they evolve beyond IMT-2000, especially with respect to mobility management and convergence with evolving fixed networks, as much as possible in cooperation with relevant bodies;
- network aspects of the convergence of fixed and wireless networks and ultimately migration to interoperable and harmonized network architectures to provide services transparently to users across different access arrangements.

In order to assist countries with economies in transition, developing countries, and especially least developed countries, in the application of IMT-2000 and related wireless technologies, consultations should be held with representatives of ITU-D with a view to identifying how this might best be done through an appropriate activity conducted in conjunction with ITU-D.

Study Group 19 shall maintain strong cooperative relations with external SDOs and 3GPPs and develop a complementary programme. It shall proactively promote communications with external organizations to allow for normative referencing in ITU-T Recommendations of mobile network specifications developed by those organizations.

Study Group 19 is encouraged to hold collocated meetings of relevant activities with those of Study Group 11 and Study Group 13 whenever possible, as determined by the study group management teams.

NOTE – Annex C to Resolution 2 (Florianópolis, 2004) gives a list of the recommendations under the responsibility of the different study groups and TSAG in the post-2004 study period.

8.3 Broadband and information security (ITU report)

This section summarizes an ITU report entitled “Birth of broadband”, issued in September 2003 (www.itu.int).

The explosion of undesired e-mail or spam, internet hoaxes and cyberattacks has highlighted the great vulnerability of users and the need for them to take protective measures. Any connection, broadband or dial-up, can be victimized in this way, but broadband is particularly vulnerable because around-the-clock exposure to the risk greatly increases the danger, by comparison with a computer which is only connected for brief periods at a time. Fortunately, tools are available which can be used to protect broadband connections, increasing their attractiveness for prospective users.

- Risk awareness

  The majority of broadband users are private users who have a low level of risk awareness. Broadband is renowned for making it easy to access information, but it may also become notorious for its vulnerability in the absence of adequate precautions and sufficient information. This could discourage potential users, for fear of endangering their private or business data.

  Public authorities and internet service providers (ISPs) can take steps to increase broadband users' awareness and improve system security, while producers of technology standards are partly responsible for ensuring an acceptable degree of network security.

- Firewall: the gatekeeper

  One effective way to prevent unauthorized access to personal resources on a computer with broadband access is a firewall (see § 2.4). This is a piece of software or hardware that acts as a gatekeeper for any communications leaving or entering the computer (or network).

  Many firewall providers offer free versions of their software for download on the web; however, the configuration of these products is often difficult for users. Some broadband providers have taken the initiative to help consumers with security by including firewalls for free as part of their home networking packages, and partnering with firewall producers to make installation procedures more standardized.

  Other kinds of software have also been developed to combat one of the most common problems broadband users face, i.e. spyware. Spyware is usually introduced to a computer in clandestine fashion via another downloaded program from the internet. File-sharing programs such as Kazaa are notorious for installing several other spyware applications on the computer during installation.

  Fortunately, free programs exist which can search for these files and eliminate them from the computer.

- Encryption

  While firewalls help deny unwanted communications, encryption (see § 2.8) offers an even better way to protect sensitive data as they sit on the computer or pass over the internet. Broadband connections can make use of various encryption technologies to help ensure the data stays private and unaltered as it travels over the internet, and can easily support encrypted communications – which usually require 10 to 20 per cent more bandwidth than the transmission of non-encrypted information.

- Laws and regulations

  The implementation of enhanced security systems, and the existence of appropriate laws and regulations dealing with this problem, will be of fundamental importance for the development of commercial and public applications, such as e-government, e-health or e-commerce. To carry out these services online, in fact, users should be guaranteed that their data will be accessed and manipulated only by those authorized to do so, that their electronic mailbox will not be the object of undesired bulk e-mails ("spam"), or that information given by certain services can be trusted, etc.

- Security and home users

  Security is also important for home users, who usually do not benefit from the controls and technical assistance usually provided in companies or government offices. Having a computer connected to the

internet 24 hours a day can be likened to having a window open: anybody can enter. Security is therefore necessary to build confidence, so that technologies like broadband can be exploited to their fullest potential and to help build an environment of trust in the global information society.

8.4 ITU-T Manual on security in telecommunications and information technology

8.4.1 2003 edition

In December 2003, ITU-T published a manual entitled "Security in telecommunications and information technology", which takes a broad look at ITU-T's work and Recommendations with respect to the security of telecommunications, as well as at the numerous Recommendations issued by ITU's Standardization Sector with a view to enabling the many players in the information society to secure their communications infrastructure and associated services.

The manual provides an overview of security in telecommunications and information technologies, describes practical issues, and indicates how different aspects of security in today's applications are addressed by ITU-T (www.itu.int/ITU-T/ publications). Following the introduction, the main subjects covered by the manual are:

- Basic security architecture and dimensions (Recommendation ITU-T X.805).
- Security framework requirements for telecommunication networks.
- Mechanisms for the security of personal data (Recommendation ITU-T X.509-PKI).
- Applications, in two parts:
  1) End-user applications
     - Voice over IP
     - Fax
     - Multimedia
  2) Network applications (service quality and integrity)
     - Network management
     - E-health

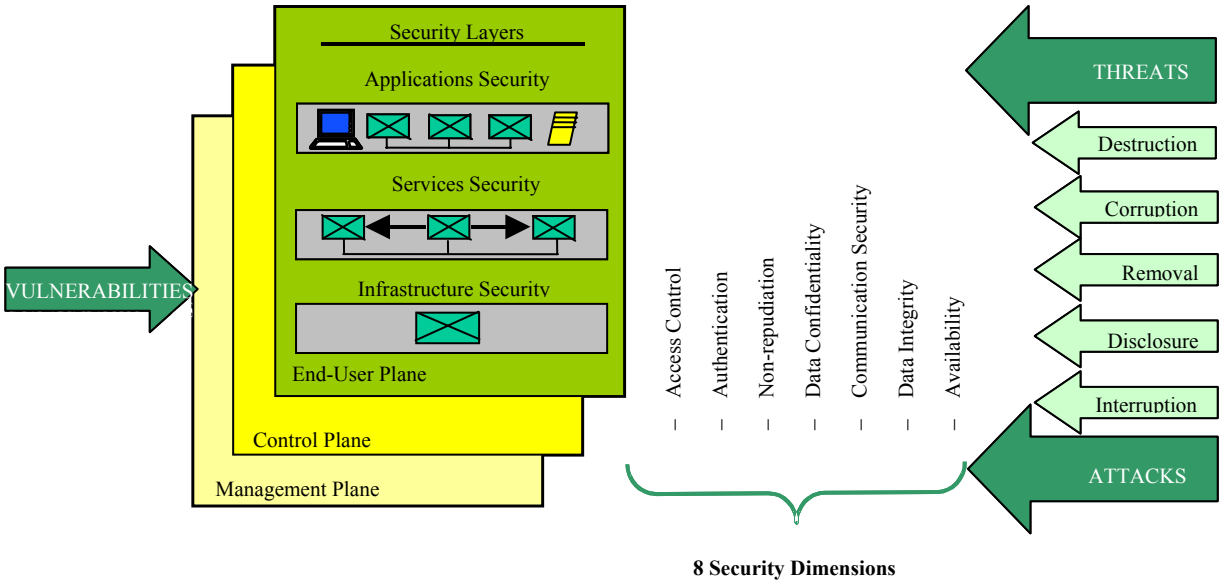
Annex A contains a list of security-related acronyms and terminology, while Annex B contains a catalogue of ITU-T Recommendations relating to security.

8.4.2 2004 edition

The 2004 edition of the manual (4 October 2004) provides a complete overview of the many ITU-T Recommendations, including those produced jointly with other international standardization bodies, concerning protection of the communication infrastructure and related services. This edition complements the one that appeared at the end of 2003, covering such additional security issues as availability and the potential for damage in the absence of security on communication networks. The manual also includes standardization work done since 2003. Of particular note is the fact that this manual, in order to do justice to the many different facets of security, defines a framework and an architecture so as to lay down a common language to allow everyone to deal with all of the concepts.

Following the introduction in section 1, section 2 introduces the basic security components and architecture as defined in ITU-T Recommendations, in the form of the eight dimensions of security: access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability and privacy. These general principles form the basis for the development of security standards for other bodies (X.800-series Recommendations).

Figure 11 – Security dimensions based on Recommendation X.805



Section 3 introduces some security fundamentals for dealing with threats, vulnerabilities and risks, and explains how those relate to the relevant standards issued by the standardization bodies.

Section 4 provides information needed to develop security resources for telecommunication networks.

More particularly, it examines the security objectives for telecommunication networks and the related services which must be taken into account to fulfil those objectives.

Section 5 introduces the very important concepts of public keys and optimized management infrastructures. These infrastructures are particularly important as support for authorization and authentication.

ITU-T has done considerable work on security for different systems and services, leading to the creation of official Recommendations. One of the main purposes of the manual is to address the application of those Recommendations; this is the subject of section 6. This section discusses IP-based voice and multimedia applications (H.323 and IPCable com), user health care and fax. These applications are described in terms of

deployment architecture and of how protocols have been defined to meet security needs. In addition, in order to provide information on security application, the needs for network infrastructure security and network services administration are listed; examples are given.

Section 7 deals with the availability of the different security dimensions and the infrastructure. These two concepts are the principal subjects of the work of ITU-T. Information is given on availability calculation and ways for ensuring availability for a transport network. This section also includes guidelines for securing transport networks.

Section 8 outlines guidelines recently approved by ITU-T on organization incidence and security incident handling. This issue is commonly agreed to be of prime importance for establishing security, given the security threats facing telecommunication and information system infrastructures.

Finally, the following are also annexed to the manual:

- a list of the relevant ITU-T Recommendations;
- a list of security-related terms and definitions used in the manual, in ITU-T Recommendations and other services such as the ITU-T SANCHO database, and the Approved Security Definitions developed by ITU-T Study Group 17;
- a list of the ITU-T Study Groups and their current work (Questions) on security.

In conclusion, ITU-T is one of the most important players providing for security needs, not only for IP-based technologies but also numerous other sectors with a wide range of security needs.

The manual shows how security solutions are available in ITU-T Recommendations both in terms of generic framework and architecture but also for specific systems and applications – which are already globally deployed by network and service providers.

The reports are available at:

http://www.itu.int/ITU-T/edh/files/security-manual.pdf and itu.int/indoc/itu.t/85097.pdf

8.5 ITU-T cybersecurity symposium (October 2004)

At all levels – national, regional and international – there is a growing need to develop, implement and promote a body of policies, standards, technical guidelines and procedures to reduce the vulnerability of ICT networks and systems to a whole range of threats and protect the information being stored and exchanged within those systems.

In the framework of its response to these concerns, the International Telecommunication Union organized a cyberspace security symposium for 4 October 2004, on the eve of the opening of the World Telecommunication Standardization Assembly (WTSA-04) in Florianópolis (Brazil). High-level representatives from a large number of administrations and computer emergency response teams took part, along with network operators and equipment manufacturers intent on assessing the current state of the security situation and discussing possible approaches for ensuring cyberspace security.

This one-day symposium was organized around four topics:

a) Cybersecurity threats – What are the issues?

b) Experiences with and responses to cybersecurity threats

c) Standards, policy, regulatory and legal aspects

d) Lessons learned and the way forward – recommended practices, approaches and projects holding the promise of improving cyberspace security.

The principal conclusions to emerge from the Cybersecurity symposium are reproduced below.

1) **The lack of adequate security in the networks, in particular the internet, is very serious and becoming worse.** This problem stretches far beyond telecommunications as computing and networking have begun to touch almost every aspect of our life. The move to a complete IP-based infrastructure will lead to even greater challenges. Without proper security, the internet may become unusable in a few years' time, especially for supporting the evolving global networked economy. As mobile phones are more and more replicating the functionality of PCs, mobile networks are increasingly susceptible to malicious attack.

2) **Security must be built-in, not bolt-on**, i.e. security must be put into the system right from the start, not as an afterthought. This fundamental principle implies the need for a non-trivial section in all Recommendations and standards dealing with communications architectures and protocols.

3) **Network Operators and Internet Service Providers (ISPs) must play their parts to combat cyber attacks through best practices and vigilance.** They cannot rely solely on manufacturers to prevent cyberattacks. Operators must make contingency plans, monitor network activities and implement early warning mechanisms. Provision of secure communication should be easy and safe for the user, e.g., a default status.

4) **There is a need to increase awareness and educate stakeholders (citizens, manufacturers, operators, businesses and governments).** Particular attention needs to be given to the security issues that are being wrestled with by developing countries. Today, security needs to be everyone's business, as computing and networking have become such an important part of our life. Security is only as good as its weakest link. There needs to be a common language for talking about legal, technical, policy and standards issues surrounding cybersecurity to converge meaningfully.

5) **Stakeholders need to share information.** The creation of CSIRTs (computer security incident response teams)/CERTs needs to be encouraged. Security manuals ("Security in Telecommunications and Information Technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications", October 2004 (110 pages), www.itu.int/itudoc/itu-t/85097.pdf and "best practice" guidelines are a step forward, as well as a code of practice for information security management (ISO/IEC 17799:2000). Today, there is a critical need for an internationally recognized Information Security Management System (ISMS) standard and this work is now underway (e.g., some telecommunications aspects are covered in recently approved ITU-T Rec. X.1051).

6) **There is a need for stronger international collaboration, cooperation and partnerships covering standards development policies and legal frameworks concerning cybersecurity.** Various initiatives exist throughout the world that will benefit from being brought together.

7) **Developing countries want ITU to take a leadership role in cybersecurity so that they can more fully participate in efforts leading to a more secure cyberspace.**

8) **Standardization needs to be a vital part of the global cybersecurity effort.** In the development of standards, security must always be put in up front.

   - There is a need for accelerated development of security standards, in particular for Next Generation Networks (NGN). ITU should lead the standardization efforts on NGN (the ITU-T NGN Focus Group has security as one of its seven Working Groups).

   - There is a proliferation of standards bodies and forums. The substantial number of cybersecurity standards available or currently under development leads to interoperability problems. ITU may act as a focal point.

   - Carriers need to reverse their pullback from standardization as the telecoms market recovers from its biggest crisis ever.

9) **There is a need to "seed" activities related to cybersecurity in those countries which to date have no cybersecurity strategy or activity.** A number of vehicles may be useful to get started, e.g. discussion groups in academia, user associations and business groups. Such low cost start-up activities can lead eventually to regional and international collaboration and partnerships, resulting in the establishment of a credible counter-cyber attack regime.

10) **Governments need to ensure that a robust legal framework is put in place regarding cybersecurity.** This includes adequate laws, policies and enforcement.

11) **Security is a goal, not a status.** Bearing in mind that security problems are mostly resulting from organizational matters, there is a need to continuously review policies, measures and procedures to help ensure that they meet the evolving challenges posed by threats to computers, networks and connected devices.

Further information is available at www.itu.int/ITU-T/worksen/cybersecurity/

A second symposium of the same type was scheduled to be held in Moscow in March 2005.

8.6 Telebiometry

8.6.1 Introduction

Human biometry (from the ancient Greek *tele*, meaning far or distant, *bio*, meaning living, and *metron*, meaning measurement) is the science of measuring the parameters pertaining to human physiology. It involves natural systems.

Where the results of biometry are used for the remote identification (i.e. in the absence of the individual in question) of the called party, this is referred to as telebiometry. The unique signs, or coded identifiers, which represent an individual and make it possible to avoid acts of theft and other fraudulent acts are collected by standardized machines.

Being more difficult to repair in the event of damage, data systems that use telecommunication networks call for standardization of the devices used to collect biometric recordings that is in line with existing standardized measurement systems.

8.6.2 Work at the global level

The *Bureau International des Poids et Mesures* (the body responsible for ensuring worldwide uniformity of measurements and their traceability to the International System of Units) laid the foundations for the ISO 31 [Technical Committee 12 (ISO/TC12) "Quantities, units, symbols, conversion factors" – www.iso.ch] and IEC 60027 [Technical Committee 25 (IEC/TC25) "Quantities and units, and their letter symbols" – www.iec.ch] standards, establishing and confirming an internationally accepted list of measurement values and expressions underpinned by agreements in all the branches of science. ISO/IEC JTC 1/SC 37 "Biometrics" is preparing new standards for biometry technologies relating to the human body in order to ensure the interoperability and exchange of data between applications and systems.

The security of the user of biometric identification systems for telecommunication requires information fields to be entered in an orderly manner in the process of elaborating security standardization. Physiological and behavioural studies have already been organized into sub-committees to provide specifications that manufacturers in the nascent telebiometrics industry need to bring products onto the market that comply with the available science to ensure the natural parameters of life are protected (safety), and that are capable of extracting and encrypting the gathered biometric data (data security).

ISO and CEI are working together on new standards, the ISO/CIE 80.000 series. CEI is also working on a new work proposal on physiological units, NWP 277.

Other international standardization organizations have also taken up telebiometry, including:

– the Biometrics Focus Group of ETSI (www.etsi.org)

– the Internet Engineering Task Force, IETF (www.ietf.org)

– the Organisation for the Advancement of Structured Information Standards, OASIS (www.oasis-open.org).

8.6.3 ITU-T activities

During the 2001-2004 study period, Question 10/17 ("Security requirements, models and guidelines for communication systems and services") examined a range of documents relating to the imminent arrival on the market of security solutions based on hardware using biometric parameters.

The consideration of the "personal privacy sphere": a spherical personal privacy sphere two metres in diameter (reflecting the ideal human form of Leonardo da Vinci) was accepted. The user of biometric systems, where a solution is proposed to identify and authenticate the user in a standardized manner, has a right to expect definitions of the security that is offered at the different levels of scale of interactions between the unique (and irreplaceable) biometric data and automatic entry on the telecommunication networks. Furthermore, voluntary identification and authentication, already possible through a form of security by consent using a digital signature based on the user's physiological characteristics, provide a range of information that can be used for security and billing purposes, making it attractive to network operators. Consensus on the telebiometric multimodal model framework was obtained thanks to the multifunctionality of these taxonomies to overcome users' fear of new technology and reassure network operators.

Framework Recommendation ITU-T X.1081 deals with the multimodal taxonomy of telebiometric operations. This Recommendation, which appeared in early 2004 after four years of work, has created scope for the emergence of a considerable number of new products in the area of secure terminals for telephony. The telebiometric multimodal model framework (TMMF) described in Recommendation ITU-T X.1081 creates, moreover, an equitable trade-off for the network user: the free citizen provides his or her telecommunication services provider with a guarantee based on biometric sciences in exchange for a guarantee, founded on the entire body of existing knowledge in the field, of the complete harmlessness of telebiometric terminals

vis-à-vis the parameters of the physical person using them. Providers of complete telebiometric solutions will soon offer telephony systems equipped with a biometric sensor and coding capability, so as to produce, on the recipient's equipment, conclusive proof of the identity of the originator sufficient for an optimum security policy. This fundamental concept of the telebiometric multimodal model framework has been called "optimum safety and security" (OS&S).

Thus, manufacturers will have an important advantage allowing them to frustrate would-be impostors by adopting this international standard: the specifications for the characteristics of telebiometric telecommunication terminals have been fleshed out. Technological solutions will obviate the need for legal recourse with patently unscientific claims, and, even more, will make it possible to separate genuine security concerns from imagined threats that have to do primarily with individual psychology or socialization (technology phobia).

In March 2004, Question 10/17 was divided into six new Questions for the 2005-2008 period, with Question QK/17 having the subject of "Secure telebiometry".

A set of appropriate technological solutions is envisioned when specifying telebiometric sensors. Q.8/17 considers that the following actions are necessary:

1) In order to authenticate the identity of each citizen, biometric data are to be collected by safe and secure sensors. ITU-T Recommendation X.1081, defining TMMF for telebiometric multimodal model framework is to be completed by the implementation of a telebiometric database for optimal safety and security.

2) Secure transmission and storage of these confidential personal biometric data is a serious risk issue. It is addressed in a Recommendation under development on telebiometric protection procedure (TPP).

3) To solve this security and privacy problem, an X.509 scheme is proposed in a Recommendation on telebiometric system mechanism (TSM) based on PKI under development.

4) Biometric sensors and processing hardware enabling the comparison of the stored biometric data with those measured at any authentication process are to be considered. Hierarchical classification of security devices is to be developed with regard to developing countries expressed requests. This implies the need for a tamper-proof hardware to be defined.

Conclusion

The telebiometric multimodal model framework makes it possible to verify the identity of a telecommunication network user in an optimum manner while respecting the basic freedoms with respect to the protection of the unique data that are conferred to the user by nature, and that are often irreplaceable.

In addition, with the introduction to telecommunication networks of an intelligent physical agent consenting to be telebiometrically identified and authenticated opens the way for the sharing of responsibility between an operator who knows how to protect the data (encoding) and a user who knows how to protect his or her telebiometrics-capable terminal device.

8.6.4 Case study: United States

In order to protect itself, the United States of America has set up biometric checkpoints at entry points to its national territory. In September 2004, 115 international airports, 14 port zones and some 50 border crossings were equipped with systems to record photographic and fingerprint information for all international travellers; some 40 million passengers annually will be obliged to undergo this biometric procedure when they present their passport to the immigration official.

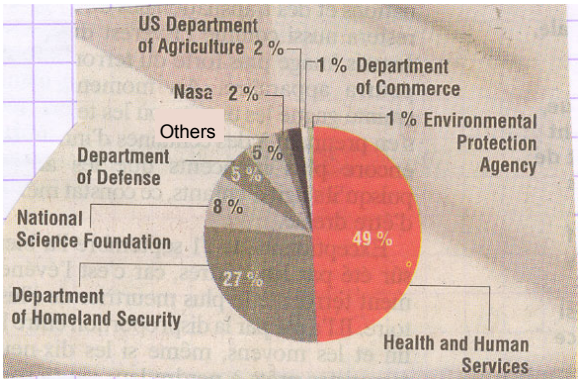
The data are immediately digitized and centrally processed. They are compared with the database in the computer assisted passenger prescreening system (CAPPS), which alerts immigration officers to any passenger considered as suspect.

The system incorporates data from some airlines and from the two most important reservation networks, Sabre and Galileo, which have agreed to provide certain information to the system's operator, the Transportation Security Administration (TSA). Others refused to do so, and difficult negotiations are currently underway between the different players to determine the exact nature of the information that carriers will be required to provide.

The inspection regime greatly increases border processing delays. In order to prevent unmanageable congestion, the government has set up a pilot programme known as "Registered Traveller". As of October 2004 it covered some 10 000 frequent flyers, who were able to cross the border almost without delay. Most of them are business people who travel outside the country for work reasons. Carrying a smart card with a chip that stores their biometric data, they typically need to pause for no more than the few seconds it takes for a camera to compare their picture with the stored data.

It is hoped that this highly computerized system, based on the interconnection of databases operated by public authorities and the private sector, will make it possible to both improve security and accelerate immigration processing. "The information held by the Registered Traveler programme will not be used for any purposes other than those of security."

Figure 12 – Funding for security research in the United States



(Percentages for 2004. Total: USD 3.4 billion)
Source: AAAS/Les Echos

8.7 Security Compendium

Study Group 17 under Question 4/17, Communications Systems Security Project, has prepared and regularly updates a communication system security compendium. It consists of three parts:

– a catalogue of approved ITU-T Recommendations pertaining to security;

– an extract of security definitions drawn from approved ITU-T Recommendations and other standards; and

– a list of ITU-T security-related Questions.

The compendium can be accessed through the Study Group 17 webpage at the ITU website (http://www.itu.int/ITU-T/studygroups/com17/tel-security.html). The compendium of security definitions allows for an overall understanding of the security terms used by the various ITU-T study groups.

9 Data transmission monitoring and acquisition centre, including IP (DTMAC)

9.1 Introduction

This section describes a data transmission monitoring and acquisition centre, including IP (DTMAC) which a national telecommunication regulator could adopt in order to secure and monitor communications against fraudulent or improper use within the sphere of its national sovereignty. The system described here is in accordance with ITU Recommendations and Chapter 5 of the *Spectrum monitoring handbook* produced by ITU-R.

A DTMAC makes it possible to process data intercepted on different telecommunication networks, regardless of whether they are uncoded, coded, compressed or protected. It recognizes the various formats of transmitted data (type of modem, IP protocol levels), provides for demodulation and reliable decoding of known and recognized formats, and performs a clear and comprehensible conversion, particularly for protocols used on the internet.

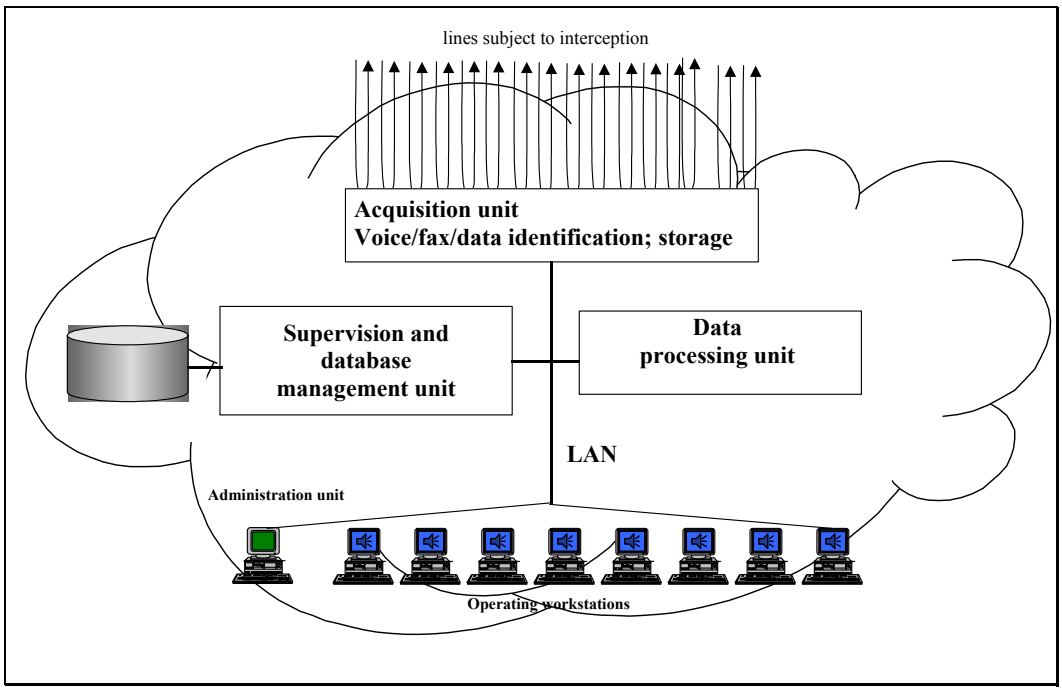
A DTMAC is an open, flexible and user-friendly system which has three main functional units (see Figure 13):

- Acquisition unit: This unit intercepts communications routed towards the DTMAC from telecommunication operators (fixed telephony, mobile telephony, cable or high-speed connection), extracts the content, converts the communication signalling information to formatted records, and classifies both uncoded information (sorted as voice, fax or data) and coded information.

- Supervision unit: This unit oversees interception operations, handles routing to centres outside the DTMAC, and handles system supervision functions (acquisition module status, event logging, administration of user profiles, statistics on the system, etc.).

- Processing unit: This unit provides access to the content by means of demodulation and decoding, and formatting of the resulting files.

Figure 13 – Schematic diagram of a data transmission monitoring and acquisition centre



The interception processing capabilities (demodulation, internet protocols, etc.) are integrated as software modules through the processing server. Consequently, it is easy to increase the system's capacity in terms of overall computing power (adding physical machines, sharing processing among machines) and the targets processed (adding a new process in the server).

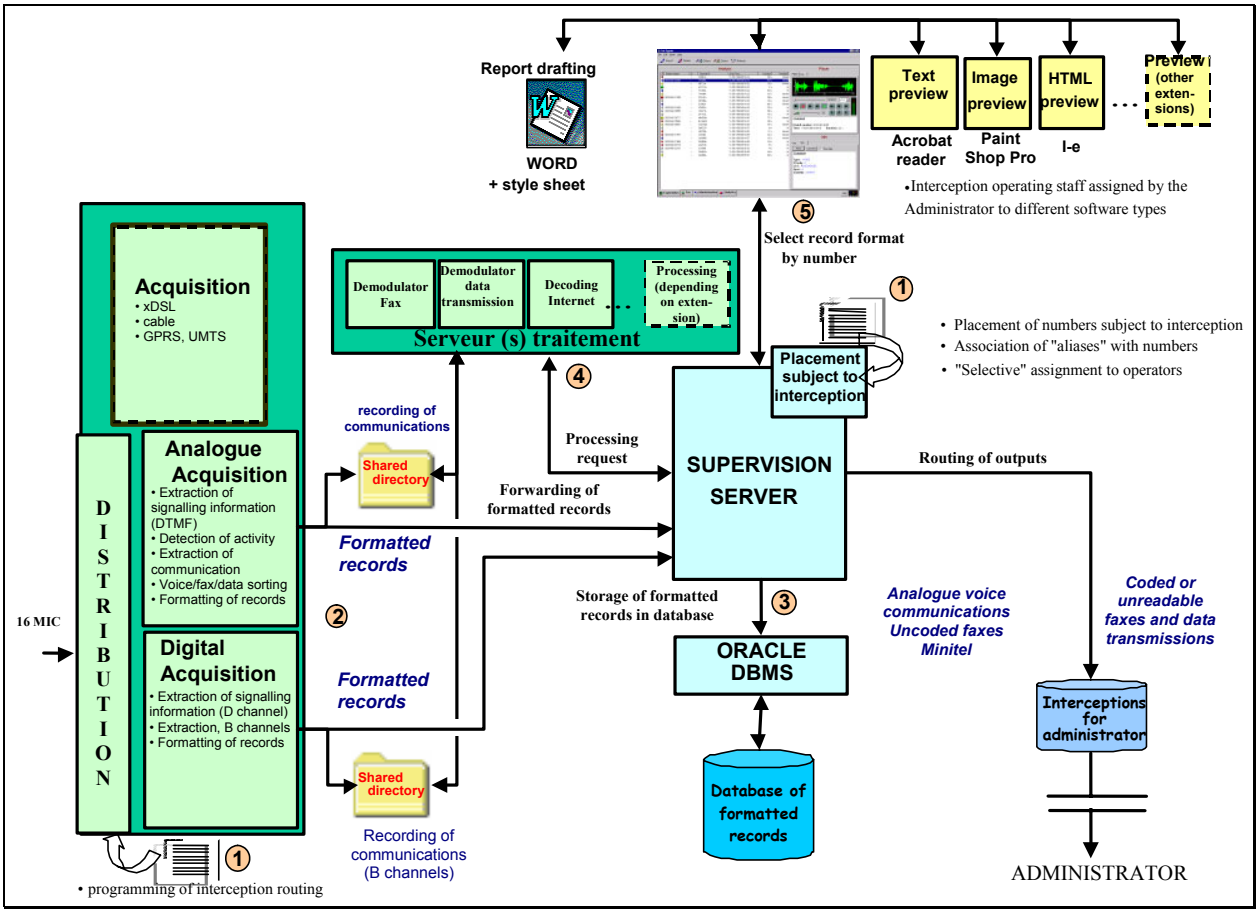
9.2 Description and architecture of a DTMAC

The principal functions of a DTMAC are as follows:

- Acquisition of communications on specific links;
- Extraction of the signalling information, converted to a formatted record;
- Determination of the type of transmission (voice, fax or data);
- Demodulation of the principal data transmission standards;
- Decoding of protocols and formats of the principal data transmission standards;
- Determination of whether the transmission is coded or uncoded;
- Local recording;
- Routing of coded transmissions to an outside body.

The architecture of a DTMAC is illustrated in Figure 14 below.

Figure 14 – Architecture of a DTMAC system



1 The heart of the system is the supervision module, a server that manages all exchanges between the system's various internal components (acquisition => processing => operation) and with external components. The operational launch of the system begins with an initial stage of configuring the interceptions, a task performed by the head of the DTMAC. He has administrator privileges which allow him to enter the numbers that are subject to interception, and the corresponding aliases for each acquisition channel, in the supervision server. He also programs the distribution of communications intercepted as transmitted by the telecommunication operator, so that they can be grouped together on an acquisition channel according to the means of acquisition used.

To complete the configuration stage, the head of the DTMAC groups together the numbers that are subject to interception depending on the various users and purposes in question.

2 At the acquisition level, the operating principle is that acquisition must be tailored to the means of communication in question, using the appropriate storage mechanisms designed for it. Each acquisition module is responsible for classifying interceptions by analysing each communication's signalling information and content (sorted by number and by identification as a voice or data communication). The content of each communication is stored, and an interception record is generated and forwarded to the supervision server containing the necessary information as to the classification and location of the communication in question.

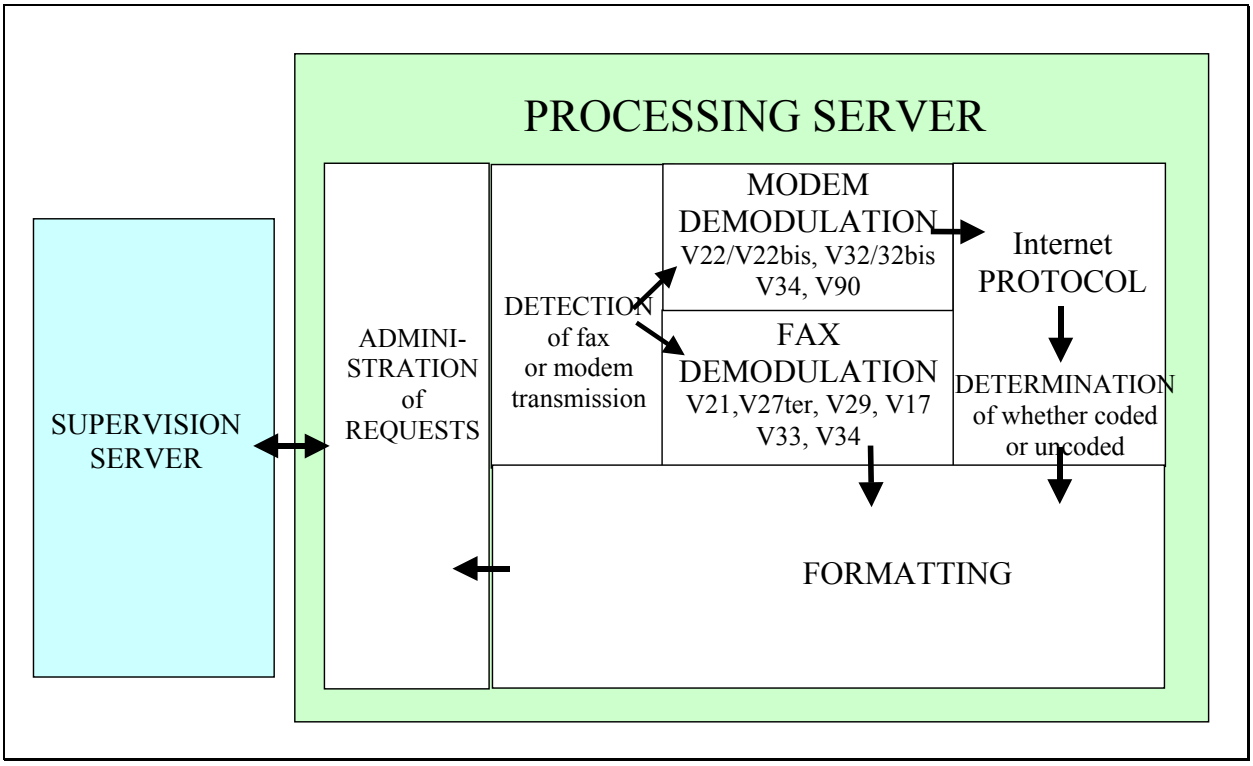
③ The supervision server places the interception record in the interception database. If the recording has to be processed in some way in order for the content to be accessed (as in the case of data transmission), the supervision module automatically engages the processing server by providing it with all the necessary information about the interception record (type of communication, location of the communication, etc.).

④ The processing server recovers the digital raw data on the communication from the acquisition module as needed, sequences the processing and sends the output data produced to the acquisition module. It informs the supervision module of the processing status.

The processing module (see Figure 15 below) offers the following processes:

- demodulation;
- decoding of protocols and associated formats;
- detection of coded data transmissions.

Figure 15 – Functions of the DTMAC processing module



⑤ The operator can then make use of files processed on the basis of the list of interceptions to which he has access.

In this shared architecture, each acquisition module (both present and future) has its own provision for storage. Sharing the storage load among the acquisition modules means that the supervision server will not saturate its own communication and storage capacity as the acquisition modules grow in number and more types of acquisition modules are added.

This choice of shared architecture enables the use of computer and network resources to be optimized and facilitates development of the system.

The DTMAC architecture lends itself to development and expansion as necessary in terms of performance, capacity and overall design:

- it makes systematic use of standard interfaces and formats (".htm" for HTML pages, ".wav" for sound files. etc.);
- it uses standard languages and an object-oriented design;
- it retains the ability for technical upgrading;
- processing is carried out using PCs, which facilitates updates and subsequent development (advanced programming workshop, widely available computer-system competencies), and it uses standard computer workstations and hardware.

This choice of architecture makes it easy to integrate subsequent upgrades without regularly having to call in the system vendor for assistance.

The choice of distributed architecture allows optimization of the utilization of IT resources and networks and facilitates system evolution.

10 Case studies

10.1 ITU

As part of the activities of ITU-T, a workshop was held in Korea in May 2002 on the subject of network security, and above all technical aspects of the securing of communication networks. The concept of "critical infrastructure" was introduced. As ITU uses the term, network infrastructures are public or private networks capable of carrying large quantities of data across international boundaries. Critical networks are those that carry national security information or highly valuable financial information. Case studies on network security and the corresponding regulatory schemes were presented from Brazil, Canada, Korea and the Netherlands.

Full information on the workshop can be found at the webpage
<http://www.itu.int/org/spu/ni/ipdc/index.html>.

ITU-T plans to hold another workshop of this type in October 2005.

10.2 Network security around the world

At the end of 2002, the French government published a document (see <http://www.cfce.fr/ntic>) describing the state of security of communication systems and networks around the world. The paragraphs that follow provide a summary of that study.

North Africa and the Near East

Given the very low rate of internet and e-commerce penetration in most countries in this region, network security issues have a limited impact and the regulatory structure, by and large, is virtually non-existent.

Sub-Saharan Africa

At the regulatory level, network security is not yet a major concern of the local authorities as their primary focus is still on establishing networks rather than protecting them.

Data encryption and coding remain rare practices, and hence monitoring by the authorities is limited.

North America

This area is characterized by a lack of restrictions with regard to cryptography and the confidentiality of communications. This situation arises out of a desire not to impede the development of electronic communication and the ICT industry in general, leaving the sector more or less free to regulate itself. Governments play a much more active role, however, in the area of domestic security. In the marketplace, technologies based on biometrics are being developed for commercial use, as are systems using cards with embedded chips. Among the security solutions now being developed in North America are virtual private networks (VPNs) and wireless local area networks (WLANs).

Latin America

For most Latin American countries, the security of communication networks is a secondary concern. International standard ISO/IEC 17799 on information security procedures has already been adopted by some standards bodies, but it has not been widely implemented in the region. There is a legal lacuna in Latin America in regard to cryptography and so these technologies are freely used.

Asia

The Asian countries are characterized by the lack of any legislative framework concerned with computer and network security. Consumers and businesses are left to use whatever security solutions they think best. Governments often lead the way by example, such as by supporting systems of the PKI type.

The security market has seen a burst of activity in the last two years. In India, the demand for more sophisticated systems has grown recently, such as for intrusion detection services, content management, identification, URL filtering, security consulting services, encryption systems including public key infrastructure (PKI) systems and virtual private networks. Demand for all of these is strong and growing.

Europe

Most European governments have become aware of the importance of telecommunication infrastructure security. Network availability and integrity are guaranteed essentially by rules imposed on telecommunication operators as part of their licensing requirements. Many countries have established or are now establishing private networks for their police forces and civil protection services. Cryptography is now in common use in the European Union's member states. The areas of highest priority now are the security of mobile communications and migration to the IPv6 protocol.

Middle East

In the Middle East, there are relatively few restrictions on the use of encryption systems. National telecommunication operators, many of which hold a monopoly, manage electronic communications using filtering systems.

Although the most modern network security technologies are available in the Middle East, they are not yet used by local firms which for the most part are content to use simple systems. Companies are only just beginning to become aware of the importance of security for their communications, as e-commerce is introduced to the region.

World overview

In an information society that is increasingly interconnected, terrorist threats since the end of 2002 have underscored the importance of ensuring that communication networks are secure. Awareness of what is at stake, which centres on economic factors, varies from country to country depending on its level of development: less developed countries are more concerned with building networks than with protecting them, while more developed countries are keen to ensure that their public sector communications are secure.

10.3 Combating spam

We have entered the age of electronic messages, with e-mail and instant messaging. Unfortunately, the main advantages of e-mail, its low cost and ease of use, lead to problems of their own. One of the most serious is unsolicited junk mail (spam).

10.3.1 Its history and definition

Spam is unsolicited e-mail. Anyone can send spam, it is easy to do and costs very little. However, few people appreciate receiving it, and even fewer know how to stop it. Spam is more than a time-waster. ISPs and mobile operators spend millions of dollars every year storing, transmitting and controlling spam. Those costs are passed on to the customers. Spam also has a negative effect on company productivity. Public administrations and businesses alike understand how important e-mail is to smooth operations. Since this means that employees are spending increasing amounts of time on e-mail, the need to make this tool more efficient and filter out spam has become more urgent.

10.3.2 A social and technical phenomenon

Spam is a social and technical phenomenon. It is social in that human beings, not computers, create spam; therefore it has more in common with the world of organic things than mechanic. The fight against spam is more than just a struggle against a software program or against computers. The fight is against an army of individuals who think and breathe just as we do. They dispose of an array of weapons deployed against us. The most powerful weapon in their arsenal is the ability to change and continually adapt their behaviour.

Spam is constantly mutating, as spammers change their tactics to get around the filters that are put up to block them. Thus, message headers bearing information such as the originator's IP address are manipulated, and the spammers regularly change their site names.

An effective filter must thus continually adapt, if it is to keep up with an agile enemy.

Since spammers constantly adapt their attack methods and change their messages, a filtering system based on a single criterion (such as the IP address or the message content) would be ineffective. Any effective anti-spam solution must be sufficiently sophisticated to deal with several variables at the same time.

10.3.3 Key requirements in the fight against spam

There are four key requirements: effectiveness, accuracy, ease of use, and performance

- The most important criterion for any anti-spam solution is its effectiveness, i.e. how much spam the filter can block.

- Another important factor is accuracy. Does the filter block legitimate messages too? For a solution to win over a majority of prospective users, it must distinguish very accurately between legitimate messages and spam.

- Next, how easy is it to use, i.e. to install and operate? Are users required to create and update their own filters? Is the solution a transparent one for the user? A solution that is difficult to use is likely to be used badly or not at all.

- Finally, the performance of the filter, i.e. its effect on speed, is important. Will it slow down the delivery of e-mail? This can be a decisive factor, particularly for the major access providers who are obliged to control and forward great volumes of messages.

10.3.4 Technical anti-spam solutions

The principal anti-spam solutions use the following methods.

a) IP address blocking

The Mail Abuse Prevention System Realtime Blackhole List (MAPS RBL) is a sort of blacklist that is being continually updated to identify domains which are known to harbour or tolerate spammers. The MAPS RBL allows mail managers to rapidly update their list of blocked domains and IP addresses and supports automatic server-based execution of those updates.

A disadvantage of the system is that it works by blocking entire domains. For this reason, the organization behind MAPS RBL is cautious about adding new names to the spammers' list. Thorough, time-consuming research is needed before deciding whether an entire domain should be blocked or not. Once a domain has been added to the spammers' list, though, the flow of spam from it generally dwindles.

MAPS RBL alone is thus not a realistic anti-spam solution. It is frequently used in conjunction with other techniques, despite its tendency to block legitimate e-mail.

b) Content-based filtering

In terms of effectiveness, content-based filtering tends to create the same type of problem as IP address blocking.

Certain filtering solutions therefore combine content-based filtering with IP address blocking. In general this involves a number of static filters, with network administrators writing their own filters. As a rule they are not updated dynamically from a central database. At best, updates may take place on a monthly basis. These solutions allow spam to be filtered on the basis of message contents, subject, and, in some cases, the sender. They are applied at the server level, and therefore obtain high scores on ease of use. However, they do not provide full spam blocking, as they also block up to 2.21 per cent of legitimate e-mail.

c) Signature-based anti-spam measures

Anti-spam protection based on spam signatures is modelled on practices developed by designers of antivirus software. By identifying and monitoring new threats, they are able to devise rules for updating filters to protect system integrity and security. The filtering rules are designed by specialized operators or computers to determine whether a given message belongs in the category of spam or not.

A critical point is the ability to monitor spammers' activities in real time. A network of decoy e-mail addresses is placed in prominent positions on the internet, where spammers are known to be active. The

spam thus harvested is automatically forwarded to an around-the-clock operational centre. In this way, new rules dealing with the latest spam can be sent in real time to update filtering software installed on the customer's mail servers.

This is a powerful solution, with the option of activating or deactivating the filtering rules depending on their usefulness at any given moment.

10.3.5 OECD's work on spam

In collaboration with the European Commission (Enterprise and the Information Society), OECD held a workshop on spam in Brussels (Belgium) on 2 and 3 February 2004. The workshop programme and presentations made are available on the OECD website.

The following points are worthy of note:

Session 1

Governments, users and representatives of the industry have a duty to identify the characteristics of spam with a view to drawing up a report on the problem and eliminating it. In addition, principles have to be established in order to quantify the efforts that need to be made in order to do away with spam, measure its rate of expansion and determine what measures have already been taken to combat this phenomenon.

Session 2

The undesirable impacts of spam are experienced by all categories of internet users, from the individual through to business users, governments, management service administrators and the providers of such services. The elimination of spam entails significant costs, both economic and social, for all of the aforementioned players. This session explored the various costs associated with spam, taking into account the principles of user protection, message privacy and network security, as set out in the corresponding OECD guidelines.

Session 3

This session focused on the new technologies and business models used by spammers, and considered the following questions:

- How do spammers obtain e-mail addresses?
- How do spammers remain undetected?
- How is a spam business conducted profitably?
- How can technologies be changed in order to block new opportunities for spammers (for example, spam via SMS or instant messaging)?
- How can new technologies and policies lead to opportunities to stop spam and increase the volume of e-mail usage?

Session 4

This session looked at the various technical solutions that businesses and ISPs can implement to combat spam.

Session 5

Examination of the laws in place in OECD member countries to regulate spam.

Session 6

Spamming is a global problem requiring a global solution. Effective anti-spam legislation is very difficult to implement. However, on the basis of existing national legislation it could be made a reality, to which end enhanced cooperation is required.

Session 7

How the best-practice use of electronic communications can minimize the impact of spam.

Session 8

A multidimensional approach is needed in order to eliminate spam.

Session 9

Determination of the next steps to be taken at the international level.

(For further details, visit the OECD webpage at:

http://www.oecd.org/document/47/0,2340,en_2649_22555297_26514927_1_1_1_1,00.html)

10.3.6 ITU workshop on spam

In § 37 of the Declaration of Principles adopted during the first phase of the World Summit on the Information Society (WSIS), held in Geneva in December 2003, the participants acknowledged that "spam is a significant and growing problem for users, networks and the internet as a whole". Furthermore, in § C5 d) of the WSIS Action Plan adopted on the same occasion it is stated that, in the interests of building confidence and security in the use of ICTs, it is necessary to "take appropriate action on spam at national and international levels".

Further to the measures adopted by WSIS, the ITU Secretary-General convened an international meeting in Geneva from 7 to 9 July 2004 entitled "ITU WSIS Thematic meeting on countering spam" (documents available on the webpage: www.itu.int/spam).

10.3.7 Global symposium for regulators (ITU)

At the fifth global symposium for regulators, held in Geneva 8-10 December 2004, one half-day was devoted to the subject, "How to combat spam?"

After reviewing the various activities undertaken by ITU and international organizations and the work of WSIS (see above), the meeting approved the following guidelines for actively combatting spam:

1) National legislation

   It was noted that few countries had effective laws in place; legal clarity on spam, depending on its nature; an administrative solution can be more rapid than one based on criminal law. Country-wide coordination with all of the players should not be overlooked. This legislation must be enforced using modern verification technologies.

2) Assessing the spam effect

   Studies, surveys and consultations of public opinion and the major players are essential to find the spammers, at the national and international level, and identify them (promotion of technical solutions).

3) International cooperation

Indispensable, particularly for developing countries, which have telecommunication infrastructures that are still under construction, therefore few or no national spammers.

As the problem does not originate within a national territory, international cooperation is indispensable, on the basis of national legislation.

The report and conclusions of the colloquium are available on the ITU site.

NOTE – Global Regulators' Exchange (G-REX).

G-REX, launched by ITU in May 2001, is an on-line forum which regulators and policy-makers can use to share views and experiences. The URL is www.itu.int/ITU-D/treg/

The site includes information for countries and regions, including outlines of regulatory agencies around the world and **anti-spam legislation.**

Conclusion

Fighting off spam effectively is extremely difficult. A successful solution requires a complex approach on several fronts, both technical and organizational, and one that, furthermore, is capable of being rapidly adapted.

Of the three methods described in this section, only the anti-spam signature method has proven itself in defeating spam.

10.4 Phishing

The Federal Trade Commission in the United States describes phishing as a high-tech scam involving "internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims."[6]

Past cases have involved spoofed e-mail messages purporting to be from a bank, written in HTML format using the bank's actual logo and address. The messages are designed to lure the clients towards false sites with an address resembling the bank's legitimate address; there, the clients are asked to re-submit their personal financial information, which thereby falls into the hands of the hackers.

The convenience of e-mail and online communications, which make them so useful for legitimate e-commerce, also makes them an attractive target for spammers and cybercriminals.

If businesses are to continue relying on the effectiveness and convenience of customer correspondence by e-mail, consideration will have to be given to making this channel of communication secure against attacks by criminals drawn by the prospect of online fraud. The response will have to make use of secure messaging, with digital encryption and signing to protect the contents and authenticate the message and sender.

What is needed is a secure messaging solution that does not require any special action by the user. Such a solution would take over the tasks of encrypting, decrypting, signing and verifying messages, as well as looking up and storing the required public keys; in short, it would be a transparent, automatic system

---

6 FTC Consumer Alert, "How Not to Get Hooked by a 'Phishing' Scam", <http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm>

working at the network level. However, for the e-mail application to be automatically secure – a precondition for it to be truly effective and become widespread – it would have to be based on open standards and provide a way to configure and maintain secure connections with correspondents who do not have secure e-mail and cannot be expected to learn how to use it.

These solutions must not only be transparent for the sender; once the addressee has been authenticated, they must provide automatic verification and decryption of e-mail, with a verified signature for any reply. To meet this need, systems have been developed that operate transparently at a network layer, using small proxy footprints at the end of the electronic message received. These systems can provide automatic e-mail security at both ends, for e-mail senders and recipients alike, with no special training.

Once this kind of system is in place, e-mail and on-line communication can go from being a major target for cybercriminals to being a safe method of communication with customers and partners, significantly reducing the potential for spoofing.

For US-related information, see www.ftc.gv/bcp/conline/pubs/alorts/phishingalrt.htm

For Australia, see www.data.gov.au/spam

NOTE – In August 2004, a US anti-spam filtering company recorded in excess of 125 000 fraudulent e-mails with the letterhead of a major US bank within a period of five hours. Faced with the world-wide scale of these attacks, banks have set up, in addition to spam filters, randomly changing access systems: security tokens that change with each session, calculators that change every sixty seconds (the system in use in Switzerland since mid-2004). Hackers have used more elaborate ruses (e.g. clicking on a URL for a site supposedly under construction) to introduce a Trojan horse. The best way to deal with e-mail of this type remains the trash basket.

10.5 Convergence of information systems, goods and persons: IP network video surveillance

The trend on security and safety markets is towards increasing convergence of resources and optimization of the systems (physical and IT alike) used to protect buildings, persons and information systems. In the past, the separate security systems (video surveillance, access control, information systems etc.) were independent and autonomous, functioning in a dedicated closed circuit. With the explosion of the internet, IP interconnection, making it possible to integrate safety systems and information systems, is increasingly taken for granted. This sharing of physical and logical infrastructure also meets the rising need for flow sharing any time, any place.

With developments such as telecommunication deregulation, the explosion in the number of sites, worker mobility and the need for real-time tracking, business has entered an investment optimization phase leading to:

– infrastructure pooling and consolidation;

– technological standardization and evolution (protocols, compression, etc.);

– need to identify major sources of savings;

– low-cost productivity gains.

The security aspect, meanwhile, is becoming ever more critical to maintain an adequate level of security for the entire interconnected system (at the system level, the data level and the transfer level). It is significant at different levels:

– strategic (for the executive);

– operational (for functional and line managers);

– technological (for system administrators).

One of the concrete applications showing how IT and video are converging is IP-based network video.

Network and broadband growth is facilitating access to new and ever more advanced applications, including video. Surveillance video systems are increasingly being interconnected with information systems with a view to infrastructure optimization.

The surveillance video world is changing radically with the transition from analog to full digital. In 2003, IP-based network video made up 10 per cent of the European surveillance video market, with turnover of some EUR 65 million, increasing rapidly (doubling every year). The situation in France today is that one in five companies possesses surveillance video cameras, and the number of new installations connected every year is roughly 600 000.

Surveillance video is no longer limited to highly sensitive sites, as it was in the past; a host of new applications (research centres, tourism, services, project management, etc.) are available that go far beyond security to provide solutions for queue control or the study of customer behaviour, for example. This brings with it growing demand from users for secure surveillance.

Surveillance video also makes possible remote monitoring, multi-site management, centralized digital recording, and integration of surveillance into access control and intrusion detection. Security managers can have real-time access to surveillance video data, while respecting the following:

– off-site (e.g. web-based) surveillance;
– system availability and bandwidth management;
– performance, reliability and quality of the real-time service delivered;
– interoperability with third-party systems (e.g. access control and biometrics);
– transparency, ease of installation, flexibility in use.

Before the network video system is interconnected with the IP information system, a careful analysis must be conducted of the risks to which the former may be exposed:

– risks associated with the protocols used (H323, SIP, etc.) – e.g. attacks against the implementation of the protocol by the installed equipment, or spoofed identity attacks;
– risks associated with the information system being used for monitoring or intercepting communications, or DoS attacks to crash the system.

Security considerations are therefore of prime importance, whether it be in:

– raising awareness to existing risks, intrusion probes, or attempted exploitation of vulnerabilities (physical or logical);
– technical audits of the infrastructures in place;
– the implementation of technical forms of protection such as:
  • patches for the equipment in use, to ensure functional surveillance;
  • utilization of SIP protocol to forestall spoofing;
  • secure real-time transport protocol (SRTP) to avoid interception;
  • intrusion prevention systems (IPS) to protect against DoS attacks (may have an impact on performance; potential for false positives).

Network video is increasingly in demand for parking facilities, urban areas, public spaces (sporting competitions, stadiums, etc.), public transportation systems, retail outlets, banks and so on. More and more businesses are looking at integrating within their single network the traffic generated by network video and access control signals and alarms.

Printed in Switzerland
Geneva, 2006

Photo credits: ITU Photo Library