Green Book on the Security of Information Systems - Draft 3.6

July 14, 1993

Contents

1 Preface

The Council adopted in May 1992 a Decision in the field of the security of information systems comprising the development of overall strategies for the security of information systems (action plan) and setting up a Senior Officials Group (SOG-IS) to advise the Commission on action to be undertaken. The action plan having as objective the development of overall strategies aiming to provide users and producers of electronically stored, processed or transmitted information with appropriate protection of information systems against accidental or deliberate threats.

The scope of the Decision foresees the following lines of action:

1. Development of a strategic framework for the security of information systems
2. Identification of user and service provider requirements for the security of information systems
3. Solutions for immediate and interim needs of users, suppliers and service providers
4. Development of specifications, standardisation, evaluation, and certification in respect of the security of information systems;
5. Technological and operational developments in the security of information systems; and
6. Provision of security of information systems.

The action plan is implemented by the Commission, in close association with related actions in Member States and in conjunction with related Community research and development actions. As a step towards the formulation of the "Action Plan" identified in the Council Decision and in accordance with the opinion of SOG-IS a "Green Book on the Security of Information Systems" is being prepared, which addresses, in accordance with the Annex of the Decision, an overall view of the

- issues involved, and the
- spectrum of measures that result from an analysis of the issues.

The present document sets out the background to the development of a consistent approach to Information Security in Europe taking into account common interests with other countries. The intention of the Commission Services in preparing the present document is to encourage a better understanding with the sector actors in the Community on Information Security issues and to develop a consensus on the requirements to be considered. It therefore does not necessarily represent the views of the Commission Services, or of the Senior Officials Group for Information Security, on the subject, but rather provides a basis for reflection and concertation with sector actors and Member States.

The "Green Book" represents an intermediate step towards the formulation of the Action Plan foreseen in the Council Decision. It is to state the main issues related to the security of information systems in its context. A deliberate effort has been made to present the subject matter in as objective a fashion as possible. By progressively widening the consultation in the preparation of the document the wish is, to obtain a representative and balanced view of the issues and the nature and implications of the options for action one may wish to consider. In its presentation the document is intentionally avoiding to voice an opinion on the framework or organisation which might be adopted to address a given issue or requirement. Such recommendations are to be included in the Action Plan.

Note on Draft 3:

The preparation of the document includes four successive phases including iterative steps in the preparation of the document:

1. Preparation of an Outline and Collection of material
2. Drafting
3. Informal Consultation
4. Formal Consultation

In its present form it relates to the result of Phase II of the preparation of the Green Book. The present draft document is the result of numerous contributions received from experts, working in the framework of IBAG, SRI, the Security Investigations and SOG-IS members (over 60 contributions received). To develop the thinking on specific groups of issues, the Advisory Group reinforced by other experts were consulted and contributed to the development of the document:

G. Axelsson
F. Iribarne Navarro
F. Piau
C. Blatchford
C. Jansen
E. Pimentel Saraiva
L. Cabirol
M. Jones
R. Pizer
D. Cerny
M. King
K. Presttun

B. Collins
S. Kowalski
M. Purser
M. De Soete
H. Kurth
K. Rihaczek
A. Eriksen
P. Landrock
G. Roelofsen
S. Geyres
O. Leiberich
R. Rueppel
A. Hallan
R. Moses
G. Ruggiu
G. Hardy
P. MAller
M. Tuset
S. Herda
A. Parondo
P. van Dijken
E. Humphreys
A. Peralta
D. Willis

Their contribution and valuable advise is gratefully acknowledged.

2 Introduction

Individual, corporate and national wealth is increasingly in the form of information. The growth and performance of an estimated 2/3 of the economy relies on manufacturing or services heavily dependent on information technology, telecommunications and broadcasting, and therefore depends critically on the accuracy, security and trustworthiness of information. This is of as great importance and interest for individuals as for commerce, industry and public administrations. Correspondingly, the protection of information in all its aspects, here referred to as Information Security , has become a central policy issue and a major concern world-wide.

The Council Decision of March 31, 1992 in the field of information systems recognises this situation and calls for the "development of strategies to enable the free movement of information within the single market while ensuring the security of the use of information systems throughout the Community".

A consistent approach at European level could help to promote the interoperability of systems, lower existing barriers and avoid the formation of new ones between the individual Member States and with other countries Therefore, there is an urgent need to address requirements and options for action in the field of security of information systems at national, Community and international level in close collaboration with sector actors and national governments. Any action must take into account both national and international commercial, legal and technical developments.

The key issue is to provide effective and practical security for information held in an electronic form to the general users, the business community and administrations without compromising the interests of the public at large.

Since information security is involved in the protection not just of property and people, but even of society itself, Member States regard it as a topic which, like defence, touches on national sovereignty.

Structure of this document

The core of the document is describing issues and requirements for action. These issues are grouped under the following headings:

- General issues. Here some of the basic issues relating to the security of information systems are described. These place security into a fast evolving world economy and treats issues like rights and obligations, human rights, openness and protection.
- Demand related issues. Issues under this section are concerned with requirements, security objectives, Codes of Practice, and the needs for digital signature and privacy enhanced communications.
- Supply related issues. The subjects discussed cover possible answers to the demand for security and include Trusted Third Parties, evaluation and R&D.
- Liability related issues. Under this heading issues relating to the consequences of security breaches are dealt with. These include civil law and insurance.

The diagram below depicts this structure.

3 Scope

4 General issues

4.1 Globalisation of the economy and mobility

Issue

The internationalisation, diversification, pluralisation and popularisation of the use of communications and information systems.

Discussion

The unprecedented increase in mobility and the provision of global communications has resulted in manufacturing, trade and leisure activities extending world-wide. Distributed manufacturing, publishing, and financial operations form the back-bone of the modern economic system. Travelling and communications for business or pleasure are common place. This is being supported, and sometimes driven, by a spectacular development in the field of communications and by the proliferation of affordable and easy to use information systems. In the last decade the cost-performance of long-distance transmission has improved by 5 orders of magnitude. This change is providing the basis for a rapid diversification of world-wide services customised to provide access to a full range of information services and utilities wherever and whenever required. Terrestrial, satellite and mobile networks provide the physical infrastructure and an unrestrained number of service applications provide the customised applications.

The nature and scope of provision of Information Security in this new world of open, multi-service and multi-media communications with a multitude of alternatives to routing, management and access has profoundly changed the requirements and options for Information Security (IS).

Requirements

- Revision of the scope and approach to information security to reflect the new conditions, challenges and requirements brought about by globalisation
- adaptation of the respective policies and regulations.

4.2 Internal Market ("four freedoms")

Issue

Alignment of the national conditions relating to Information Security with the conditions of the Internal Market

Discussion

The Internal Market provides for the "four freedoms" within the Community, ie free movement of goods, capital, services and people. The legislation of Member States provides for the internal needs for Information Security, however the requirements in the case of trans-European communications remains to be addressed. Inconsistent or incomplete provisions of information security represents a technical obstacle to the working of the Internal Market.

Requirements

- Verification of the existing provisions with respect to their conformance to the Internal Market Policy of the EC implying the removal of existing internal barriers and the avoidance of the formation of new technical barriers due to divergent application of IS rules, regulations and legislation
- provision of IS to business and the public of solutions freely applicable throughout the Community and on a preferential basis at the international level.

4.3 Human Rights and the protection of communications

Issue

To reconcile the human right to privacy and the obligations of law enforcement to protect public order.

Discussion

Privacy and the protection of private information is considered one of the fundamental human rights of citizens and is protected to varying degrees in Member States. The European convention on Human Rights states "Everyone as a right to respect for his private and family life, his home and his correspondence". Citizens have the legitimate expectation that this right is respected and that solutions are made available to him that ensure the safeguard of this right. This applies to conversation in the home and to a lesser degree when telecommunications is being used. However, prevailing national solutions do not, at present, provide for trans-European services and communications and this lack can be exploited, inter alia, by organised crime. With the rapid growth and diversification of communication services the rights and duties of citizens and law enforcement are being reviewed and redefined, eg FBI supported legislation and the proposal of the government to provide US business and citizens with cryptographic devices including explicit provision for intercept by law enforcement agencies.

In this context, it should also be noted that the Maastricht treaty establishes a citizenship of the Union, and that every person holding the nationality of a Member State shall be a citizen of the Union.

As the safety and security of the citizen provided by the process of law and order is also related to human rights, reconciling these objectives represents a delicate political issue.

The diagram below gives an overview of international, Community and national responsibilities for different application categories.

Requirements

- Definition of a common approach defining rights, responsibilities and duties of citizens and business on the one hand, and that of the authorities on the other hand.

4.4 Social acceptance of identification methods

Issue

To reconcile the human right to privacy and protection and the use of identification methods to control human access to systems, buildings, offices and other physical environments.

Discussion

The use of biometric methods is becoming more technically feasible and cost-effective as an identification technique for access control. Such methods rely on a system of machine recognition of a set of personal characteristics to verify the identity of an authorised user in order to allow access to some physical environment. Such personal characteristics include hand-written signatures, fingerprints, voice prints, machine phrenology, lip prints, response of the skeleton to a physical stimulus, hand geometry and retinal patterns.

Many other different personal characteristics and recognition techniques are being investigated by researchers. Some of these effect the human right for privacy more than others and some are socially unacceptable.

As an example, the retinal blood-vessel pattern of a human eye (retinal vasculature) is highly characteristic of the individual. A typical system might work as follows. The individual is required to look into an optical device and through a process of optical adjustment fixate on a crosswire whereby the recognition machine will locate the fovea of the individual, and scanning with a low intensity infra-red beam detect the nodes and branches of the retinal pattern falling within the scanned area. The measured pattern is compared with the stored pattern of the individual and access is granted or denied depending on the result of the comparison. This method of machine recognition may or may not be considered sociably acceptable on the grounds of hygiene, due to the type of information being stored about the individual (a record of which may be built up which may reveal other information relating to a persons health condition) or the general problem of protection of medically relevant information.

There are systems under trial for the recognition of human profiles eg the human face. Again these systems may not in general be socially acceptable and the issue of privacy and human rights may come into play.

Progress in bio-technology raises new questions as to the definition of privacy and as to the rights of the individual over information relating to his person and the assurances required for its use. Information relating to genetic defects are of obvious sensitivity and implies corresponding measures for protection. Work may need to be undertaken to set out a clear definition between things that are biometric and things that are medical. At the present time there is low confidence by the general public in the honesty of commerce or government in the field of bio-technology.

Requirements

- Clarification of the ownership and privacy issues surrounding biometric data
- development of an agreed classification of biometric data and conditions requiring secure handling of such data
- development of a common approach defining the rights of and responsibilities of citizens, business users, corporations and administrations using biometric techniques.

4.5 Human Rights and the safety of systems

Issue

To reconcile the human right to an expectation of the supply of goods and services that are not life threatening with the vendors commercial needs to supply goods and services that exploit information systems in safety critical functions.

Discussion

Security critical systems differ from security critical ones in that if they fail death or serious injury to people may result. The law treats the liability of suppliers in this situation differently from that where information is lost or property damaged. Suppliers are held strictly liable. Codes of practice for the development of safety critical systems exist in order to reduce the chance of failure and design techniques are invoked to analyse all possible hazards. Nevertheless risks remain.

At a community level, harmonisation of such codes of practice and design techniques would enable citizens to have greater expectations of their own safety in any member nation, and it would reduce the costs of development of codes of practice and design techniques in each nation. Furthermore, pan-community procurement would be facilitated, as would the development of safety critical systems by community wide consortia.

Requirements

- Review of current design practices and codes of conduct with the aim of generating a community wide standard for such processes
- study the legal environment within which vendors and users of safety critical systems work, with the objective of harmonising that environment.

4.6 Management of openness and protection

Issue

Openness and protection are partially contradictory user requirements, which need to be reconciled depending on the specific circumstances. The user must be able to define the security controls based on need, consistent with national, international and regulatory constraints. These controls need to managed in a way that provides protection in an open environment.

Discussion

In considering management, one must introduce the concept of a user of an Information System, and the role that they perform in using that system. At any time the user of an Information System will be performing a role, which could be one of: system owner, administrator, auditor, investigator, data provider, reviewer/collator. It is quite possible for the requirements of these roles to be logical in conflict with each other. Openness of access may be in conflict with protection from general availability. There may also be national, international or regulatory constraints which impose role requirements beyond those needed to satisfy the operational use of the Information System. An Open environment must be provided with controls that are capable of providing protection without technical limitations.

A single, isolated computer may be effectively protected, as far as confidentiality is concerned, against threats from outside by physical separation and human administration. This does not apply in the context of telematics. Telecommunications and telematics applications are increasingly being designed for maximum openness and inter-operability since the utility of ITT&B-based services and applications depends largely on the possibility of users world-wide being able to freely inter-operate over communication links. Major international efforts are underway to establish standards permitting this, in particular through OSI (Open System Interconnection), (ODP) Open Distributed Processing and ONP (Open Network Provision).

The acceptance and use of telematics services depends on meeting the justifiable interests of all parties: in particular to be able to chose trade-offs between "openness" and "protection".

In recognition of this, increasing attention is being given to the provision of Information Security Services and Techniques.

The comparison with the way this dilemma is traditionally addressed leads to some observations which most likely will also apply when information is handled electronically. These include, for example:

- The User/Originator requires the freedom to decide over the degree of openness/protection depending on his appreciation of the requirement or the applicable rules of conduct for the given activity.
- Profiles exist setting out the needs of both openness and protection that need to be supported. A single level profile will not support the requirements of all the users involved, and there may need to be mechanisms which allow for negotiation between profiles to determine temporarily agreed common profiles.
- Infrastructure, services, applications and organisation have to be adapted to provide the openness/protection.
- To the role holders, both the visibility of and the transparency of the degree of openness/protection is crucial.
- Accountability for the application of appropriate levels of openness/protection require objective records, which are themselves protected.
- The management of the openness and the protection of Information Systems requires the definition of security domains. These correspond to the security policies which are in force for the Information Systems in use, as modified by the constraints of the role holders. It should be remembered that computers which are not directly under human supervision may form part of the security domains involved.

Requirements

Development of a generic framework for the management of open and protected communications in a user/business oriented environment:

1. Reinforcement of the options to define security domains

   Terminal users, servers and other computer based resources link into business processes to provide information domains which require corresponding security domains. Such facilities must not only promote the correct degree of openness , but must also provide filters against unauthorised access. This needs to be possible not only at one site eg on LAN-Based applications, but also via MANs and other communication-links. The definition and management of such security domains needs to be possible either from within the user group or provided by a trusted third party. Virtual Private Networks have some of the features, but these would also need to be available in the context of public network based applications.

2. User Interface for the management of openness/protection

   The normal usage requires the ability to communicate either with specific correspondents, a select group, an open group or indiscriminately. The choice being determined by the nature of the information, its function and the applicable rules. The user-interface needs to cater for this as well as the underlying services and applications.

3. Objective records and procedures for the accounting of open/protected transactions

   Processes must be available that provide non-refutable evidence of the origin of, and delivery of, information to all involved partners.

4.7 Common concerns of commercial and national security

Issue

Information Security is a common concern of business, administrations, citizens, law enforcement and defence.

Discussion

Though not to the same degree, commercial and personal information security shares many aspects with the defence and other classified governmental affairs. This provides an opportunity for commercial and personal applications to build on experience and expertise from the defence and classified government area.

The reverse is also true. As commercial security advances and becomes available at a large scale, governments and defence organisations are well advised to take into account this body of experience. In addition governments themselves are, of course, in the need of adequate protection of their non-classified information and will wish to make use of public services of this kind.

Requirements

- Concerted effort to address the common requirements of business, citizens and authorities to adequately protect commercial and personal information and its communication

- definition of common rules and procedures distinguishing the handling of classified and commercial and personal information.

4.8 Security and law enforcement on international scale

Issue

Crime is exploiting weak information security to further its ends. Strong information privacy may also be used to escape investigation by law enforcement.

Discussion

Crime, and here organised crime and terrorism in particular, are relying on weak information security to prepare and execute their operations. As quite powerful means for information security have been published and are freely available, their increased use in protecting such operations is a growing problem. Public authorities have in the past used legal and regulatory powers to restrict the use and dissemination of related technologies. With the growing availability of computing power and open networks, this approach is getting less effective, as organised crime, contrary to the legitimate user, is not concerned with the use of products that are not authorised. The overall result is that business is seriously constrained in meeting its security requirements, particularly in international communications and in its relations with other organisations. If business requires the legal and regulatory powers to relinquish total control over these security related technologies, business has a "duty of care" to manage and control their use for their commercial and business purposes, including the policing and auditing of management environments.

Requirements

- An effective, internationally agreed, economic, ethical and usable solution to meet business, administration and personal needs including mechanisms for authorised interception and reporting of incidents and crimes adjusted to the conditions of the Internal Market, and to include the necessary equipment and software, but also an infrastructure of Trusted Third Parties. This will discourage "home-made" or other solutions.

4.9 Economics of the security of information systems

Issue

The use of information security impacts on costs, performance and availability.

Discussion

The cost of security is an integral part of cost of ownership of an information system, ie namely that without security the users system is at risk. The cost of protection against breaches of security needs to be commensurate with the costs (both direct and indirect) that may be incurred from a breach in security. A security breach may have short term (and perhaps, localised) implications such as loss of sales and revenue or fraud or theft. It may also have longer term (and wider) impacts on business communities through loss of confidence and consequential loss of business.

The costs of detection, resistance and recovery can be both tangible and high, and although there are techniques available to quantify risks there are no generally applicable methods for estimating the potential costs arising for example from denial of service or loss of integrity. The provision of security measures may also make it harder to use and may constrain overall performance. However, where the security risk is high enough to cause an unacceptable level of compromise, leading to considerable commercial and financial loss, then security measures must be given high priority commensurate with the nature and value of the business in question.

If IS is to expensive, clumsy, not effective in the context of actual usage or not available in time its use is avoided and high risks are taken until something drastic happens. The issue for IS is therefore, not only to be effective but also to address other requirements which impact the acceptability and application of IS.

In particular, countermeasures may have to be put in place that meet specific regulatory or legislative requirements, with associated mandatory assurance needs.

To a business, securing information can be thought of as being like an insurance policy - the cost of protection must be balanced against the likely consequences of the perceived threat occurring. This cost is made up of a number of elements, including:

- the life-cycle costs of implementing the countermeasures in relation to likely and worst case
- impact on business performance
- liability of management for incidents and relationship with customer confidence.

Requirements

- Development of an approach to a "cost of Security" model for a business and the private user. This includes, among other potential costs, the cost of installation, operation, maintenance, up-grade and insurance premiums as well as direct financial losses due to breaches of security.
- Definition of IS as business and marketing factor.
- Codes of practice and other recognised regulatory norms need to be developed which identify to a level acceptable to both insurers, regulators and the commercial courts specific duties and responsibilities of the parties to the use of Information Systems and their security requirements.

4.10 Social recognition of information crime

Issues

Negligence, ignorance and recklessness are the some of the causes of many security events and create the opportunity for information crimes.

Discussion

IS-incidents, like failures to observe safety rules, can in many instances be attributed to a lack of motivation. This is compounded by the fact that the loss of immaterial goods, for example information, is not considered as serious as the loss of material goods. This is due in part to the fact that electronically stored information can be reproduced at close to zero costs without the loss of the original. Stealing information is therefore often considered as a gain for the thief without a loss to the owner. It is perceived by many to be a game rather than a real problem because people are unable to relate the electronic world to the real one. This has the double effect of enciting negligence by the owner of the information and little concern for the illegal acquisition of information. Because of the widely practised back-up of information resources, this applies even to the intentional or accidental destruction of information.

There is much work in establishing and reinforcing "ethical principles" as applied to specific actions of information ownership, creation, dissemination, etc. These need to be related to sector actors, their control perspective and the assets over which they exercise either explicit or implicit authority. This needs to be related to codes of practice and conduct, legislation and regulation to establish the extent to which protection is dependent upon a formal or informal control environment or can rely on the enhancement of ethical and professional standards. At the moment there are no effective professional standards in IT, anyone can do IT by buying a PC and taking a bulletin board subscription. Changes to traditional programming techniques have made it possible for non-IT professionals to deliver programming and systems analysis methods. In many SMEs such work would often be done by non-IT professionals.]

Two examples of computer crime illustrate the diversity of situations which may arise:

1. In a German company (belonging to the "Association for Security") a programmer - unsatisfied with his salary - caused damage by a specific computer-programme. This program modified the data of a data bank by randomly controlled accesses. The programme was intricately hidden among other programme-parts. Within two years the data-bank became more and more defective and damaged. The costs of damages and of reconstructing the data bank were about 500 000 ECU.

2. In an office of the German Government a huge computer-system, comprising various storage means and terminals was installed. Suddenly the computer-execution-times and the response times became much longer than expected. After a difficult investigations it turned out, that a programmer, who had founded together with his wife a shop for sending out photo-equipment, has done his complete accounting, mailing, etc. for his shop on the computer in a hidden area. He had camouflaged or suppressed the protocolling of this programme. He caused damage of about 100

000 ECU.

Requirements

- Development into basic education of the Information Security requirements and concepts needed to operate safely in the Information Age
- clarification of "Info-Ethics" for the professional and individual user in its relationship to Information Security
- clarification of responsibilities of the sector actors in general and in their relations within each other, with particular reference to open and distributed applications.

4.11 Safety critical environments

Issue

Protection of information in safety critical environments.

Discussion

Safety is defined in terms of hazards and risk. A hazard is a set of conditions (a state) that can lead to an accident, given certain environmental conditions. The analysis of the safety environment involves identifying the hazards within a safety critical environment and then either verifying that hazardous states cannot be reached or that the risk is acceptable. Risk is defined as a function of the probability of a hazard occurring, the probability that the hazard will lead to an accident, and the worst potential loss associated with such an accident. You can diminish risk by reducing any or all of these factors, and there are environmental-safety techniques that focus on each.

There is an increase in the use of information systems within various areas of application which are considered as part of a safety critical environment. For example in the area of healthcare (eg medical databases), air traffic control, transportation of hazardous and dangerous goods, industrial processes etc. The increased reliance on electronic information in these various areas of application specifically related to the control and management of safety, has resulted in an increased need for the protection of the information system supplying such information. Therefore the protection of information systems used in safety critical environments is factor to be addressed when considering hazards and associated risks in such environments.

Consideration needs to be given to the common requirement of security and safety, common methods for analysing the threats, vulnerabilities and hazards, and the role of security evaluation for safety-critical systems.

Requirements

- Development of a common approach to the handling of security and safety critical requirements
- development of a common methodology for threat, vulnerability and hazard analysis for the protection of information systems used in safety-critical environments
- generation of common methodology for the design, development and procurement of safety critical systems, covering project management, development environment, auditing of process, configuration management and change control
- development of a common approach to security evaluation of information systems in safety-critical environments.

4.12 Embedded systems

Statement of Issue:

Increasing use of computers and information processing is occurring in a manner that incorporates information/computers into other products to make those products more usable, flexible, etc. These embedded systems depend upon the accuracy of the programs they contain and the information inputs/outputs to preserve the usefulness of the products in which they are placed. Failure of the processor or corruption of the programs or information contained may cause failure or destruction of the device or hazard to the user.

Discussion:

Embedded systems are already being used in automobiles for controlling ignition and carburetor systems or braking systems, in television sets and VCRs, in microwave ovens, and so on. As embedded systems proliferate they create potentials for physical hazard to users beyond simple loss of the functionality of the devices in which they are embedded. The potential will also exist that such embedded systems could constitute a hazard to the well-being of bystanders or property. For example, one scenario of embedded systems would have them in household appliances and include the capability to communicate potential failure information to maintenance providers. The potential exists that such a device could fail in a mode that would put household or service providers' telephone systems at risk.

To some extent, liability laws will cover product failures which create damage to users. However, there may need to be some added means of ensuring the reliability of embedded systems and the integrity of the systems as they leave the factory. These means may include:

Requirements

- Development of methods of testing that enable standards of reliability to be ensured, including tests to destruction where appropriate
- development of an approach for the certification of samples
- definition of requirements for fail-safe system architectures and implementations
- definition of anti-tampering and protection specifications and standards.

5 Demand related issues

5.1 Agreement on security requirements for enterprises

Issue

Identification of real world security requirements and objectives for business and administration.

Discussion

The protection of information systems must be all embracing. Consideration must be given to requirements from the view point of the enterprise, taking into account corporate and organisation plans, goals and strategies of the business or administration. Requirements at this level can be then translated into "Security Objectives" - why the security functionality is required as it applies to the operation of the business or administration environment.

These security objectives need then to be supported by a definition of the security functionality and related services required necessary to support the user/business.

The security model has not included legal, accounting or regulatory requirements which may be imposed upon enterprises rather than forming any integral part of the Enterprise requirements. Given the complexity and diversity of user/enterprise requirements for such protection it is necessary to classify the requirements in some structured way consistent with real world business and operational environments.

The protection of information systems needs to consider the enterprise requirements of the "business". These requirements not only include functionality that is "owned" by the enterprise but must include inter-enterprise requirements as well. It must consider the functionality and assurance of IT building blocks, end user applications, integration enablers (such as electronic mail), operating systems, communication services and protocols, and basic hardware and software platforms.

The balance of functionality (what it does) and assurance (how well it does it), both generic and application specific, will determine the extent to which electronic information systems are accepted as an integral part of both the public and corporate IT infrastructure to underpin business actions.

The prime requirement for any secure system must be a set of architectural principles that can be effectively translated into an overall design framework. Secure systems must be created at different "grades of assurance" from a set of policies, standards and procedures.

Specific security requirements relating to open systems will come from a threat assessment and risk analysis which will form part of the overall system security policy process.

The cost of security is an integral part of the cost of ownership of an IT system ie namely that without security the users system is at risk. The cost of protection against breaches of security needs to be commensurate with the costs (both direct and indirect) that may be incurred from a breach in security. A security breach may have short term (and perhaps, localised) implications such as loss of sales and revenue or fraud. It may also have longer term (and wider) impacts on business communities through loss of confidence and consequential loss of business.

The costs of detection, resistance and recovery can be both tangible and high, and although there are techniques available to quantify risks there are no generally applicable methods for estimating the potential costs arising for example from denial of service or loss of integrity. The provision of security measures may also make it harder to use and may constrain overall performance. However, where the security risk is high enough to cause an unacceptable level of compromise, leading to considerable commercial and financial loss, then security measures must be given high priority commensurate with the nature and value of the business in question. Sectoral requirements vary widely, as do requirements by size of enterprise within a sector. Sectoral requirements may be varied by regulation, bilateral international agreements, general trading agreements or conventions.

Increased demand for Electronic trading from all kinds of businesses, both public and private sector, will place requirements for security on the communal service infrastructure that provides the capability for such business activities. The regulatory and legal environment within which such service organisations work will become a factor for economic growth in the community, and security of service provision an element of such services.

Requirements

- Development of a taxonomy and directory of user requirements and security objectives derived from real world business applications.

5.2 Agreement on security requirements for individual users

Issue

Identification of security requirements and objectives for individual users.

Discussion

The individual user, in their role as a private citizen or as a member of a liberal profession (eg a lawyer or medical doctor), has a natural interest, and sometimes a legal requirement, to protect some of their information. Unlike in the case of the enterprise, the individual user will not normally go through a systematic process of establishing goals, definition of security objectives, etc, unless they are subject to professional standards of conduct.

The individual normally has at his disposal a PC (or small network of PCs) and some communication links, eg telephone, fax, e-mail. Physical security is likely to be weak.

Most liberal profession work under some codes of practice or conduct. These codes are of a general nature and do not normally specify particular security arrangements.

The common and specific requirements of individual users, with regard to the protection of their computer installation (physical and electronic), the protection of their data (against accidental and deliberate loss) and the protection of their communications (eg signed communications, privacy enhanced communications) must be established.

Requirements

- Development of user profiles identifying standard types of users together with typical requirements.

5.3 Security objectives for enterprises

Issue

Definition of Security Objectives for enterprises.

Discussion

Security objectives are related to confidentiality, integrity, availability, legality and auditability. Controls are related to segregation of duties and methods for obtaining independent audit of the achieved results of an Information System. Controls may also relate to the reasonableness or plausibility of information or an activity.

A security objective is a description of what security the enterprise is trying to achieve eg why this security control/function is wanted. It is a mission statement of the user/enterprise which describes why an aspect of security is needed. It is a user/business target or purpose to which security is being addressed. For example, consider the subject of data integrity and the objective "Prevent unauthorised modification to data". The security objective has the objective "Appropriate mechanisms should exist to preserve the integrity of data". For example this may be related to data held on a medical database, on a company financial database, in airline reservation system or a geography information system.

Security objectives are thus concerned with the preservation of information with regard to its utility, availability, authenticity, integrity and confidentiality within the enterprise and between enterprises or concerned with some user environment. These are dependent upon more detailed definitions of business control being made. The structure and organisation of the specialist accounting functions in a business are examples of business controls.

The organisation of security within enterprises in terms of business control structures or in the case of some user environment (eg legal, accounting, audit etc) and functions (eg IT, human resources, insurance) needs to be integrated with a set of security policies, standards (both public and in-house), and made compliant with laws and regulations (eg computer crime manual), guidelines and codes of practice etc.

The process of producing a security policy requires the use of a set of security methodologies, tools and evaluation criteria. For example risk analysis methods, baseline controls, and evaluation criteria (eg ITSEC, Federal Criteria etc.).

Security objectives thus encompasses a set of objectives (and possibly sub-objectives) and a set of related issues that reflect specific points of concern, problems, questions relative to business requirements, controls and applications.

The diagram below shows the relationship between Security objectives, Security organisation, and Security methodologies. Laws apply to the user environment directly. Their presence generates some of the security objectives. Standards may be both mandatory and discretionary, and may incorporate methodologies. The final box covers security methods and techniques.

5.4 Sectoral specifics

Issue

Beyond the normal requirements common to different business sectors and user environments there may also be additional requirements and priorities specific to the operational nature and commercial mission of a particular business. These specific requirements can be normally expressed in terms of codes of practice and baseline controls.

Discussion

Legal and regulatory provisions can be supported by Codes of Practice to achieve due care and diligence. There are those of general application and those that are industry specific. A general Code of Practice may achieved by the establishment of a security management handbook, maybe based upon the approach taken for achieving a Quality code of practice (ISO9000). The application of IS is a prerequisite for the successful conduct of business for particular sectors, especially when these sectors a highly interactive. The most prominent among them are:

- Finance
- Trade
- Medical
- Telecommunications
- Administrations.

Requirements

- Development of a set of codes of practice and baseline controls addressing specific business sector requirements.

5.5 Security methodologies

Issue

Selection of security requirements analysis methodologies (eg risk analysis methods, codes of practice etc.) and related safety hazard analysis methods relevant and applicable to the user/enterprise business policies and controls.

Discussion

Any security policy formulation must derive its requirements statement from an assessment of the potential threats against the business and the supporting service infrastructure of the IT and telecommunication processes. This will allow an eventual implementation with clearly understood trade-offs, administrative and technical measures against human malefactors, and a balance between security cost and level of operational fitness; these are components of a Risk Management strategy. The risk management strategy on a European level should be based on a rigorous and consistent approach to the analysis of the threats to and vulnerabilities of the system and its components, and where appropriate safety hazards. This approach should be based as far as possible on existing, and, possibly, standardised, risk/hazard analysis modelling techniques and products. The issues include:

- adequacy of present risk assessment techniques

- awareness about current trends, and modelling
- awareness of the responsible security officers about security
- security breach incidents
- safety hazards as they impact on or are related to the security of a system and vice versa.

Requirements

- Development of evaluation criteria and guidelines applicable to the selection of security requirements analysis methodologies (eg risk analysis and management methods, products etc)
- harmonisation and standardisation of a European and international approach
- integration of security and safety methodologies where appropriate to provide a coherent framework for the analysis of assured systems.

5.6 Security domains

Issue

Openness and protection.

Discussion

In practice, the level of IS is dynamically adapted to a given situation. This leads to the concept of Dynamic IS Management and the need to be able to define domains, in which IS is applied homogeneously.

Security Domain Concept

Domains are user groupings sharing some of their functions and support. For some activities they operate as virtually closed user groups, but have the possibility to interwork with other domains as long as certain minimum requirements ensure no loss of trust or a transparent downgrading.

The notion of a security domain is therefore important for two reasons. Namely,

- It can be used to describe how security is managed and administered, and
- It can be used as a building block in modelling security relevant activities that involve elements under distinct security authorities.

Examples of domain activities are:

- accesses to elements (eg a database for network management)
- a communications link
- operations relating to a specific management function
- non-repudiation operations involving a notary.

Security Policy

The organisation of security within enterprises in terms of business control structures or in the case of some user environment (eg legal, accounting, audit etc) and functions (eg IT, human resources, insurance) needs to be supported by a set of security policies, standards (both public and in-house), laws and regulations (eg computer crime manual), guidelines and codes of practice etc.

The security policy defines what is meant by security within the domain, the rules by which security may be obtained to the satisfaction of the security authority, and the activities to which it applies. The security policy may also define which rules apply in relations with other security domains in general, and in relations with particular other security domains.

Requirements

The management of inter-domain openness and protection may be different depending on similarities in purpose, and agreements will be needed to achieve appropriate levels of assurance. Mechanisms by which TTPs achieve efficient, coherent management of policies, procedures and controls between domains need development:

- generation of guidelines for domain creation, management and control
- development of a common framework for domain interworking
- agreement on management, TTPs, accreditation, auditing and relations with law enforcement agencies.

5.7 Information labelling

Issue

Transfer of information between domains requires agreement on the syntax and semantics of information labels, and of the procedures and mechanisms for handling labelled information.

Discussion

The information label is a short hand way of expressing the protective measures that should be applied to the labelled information.

Information labelling is an essential part of ensuring that information objects receive the appropriate level of security protection both within and between security domains.

Trust between organisations depends on the assurance that information will be handled in a way consistent with its security requirement in terms of confidentiality, integrity, availability and non-repudiation.

The need for comprehensive labels has become acute because of the increasing degree to which organisations interoperate electronically. This has led to increased reliance on technical measures to achieve adequate security. It is quite feasible for trusted systems to switch on or off technical measures automatically providing that the label adequately expresses the security requirement associated with a piece of information. Labels could then be used to make decisions on information routing, transmission enveloping, requirements for confirmation and so on.

Organisations have to agree on the range of options that do meet any particular security requirement. Part of the solution to the handling of labelled information lies in the development of Codes of Practice specifying procedures and mechanisms. There is also a need for accreditation and audit of communicating partners. The introduction of independent third parties avoids the pairwise interactions that would otherwise be necessary to establish trust.

Requirements

- Code of Practice for information labelling.

5.8 Access control and authenticity issues

5.8.1 Access control

Issue

Access control procedures to many systems are not standardised or well managed.

Discussion

Computer systems and services impose control procedures on persons (or other systems) attempting to access them directly or over local or wide-area networks. These access control procedures apply to "connections"; that is, they determine whether or not a connection, association or session is allowed to be established. These control procedures have been often primitive and relatively insecure, as the occurrence of "hacking" demonstrates.

For example, the only protection afforded may be by a password, transmitted over the network "in clear" so that any wiretapper with physical or electro-magnetic access can read it.

The requirement for secure access control is not confined to access to host computers by persons at terminals. Reciprocal (mutual) access control is often needed between two (or sometimes more) systems. Access control can apply across general telecommunication networks, determining (for example) who may call whom by telephone; or who may receive which programme on a cable TV network. In addition to applying to end-to-end (trans-network) communications, access control also applies to users and (even more importantly) operators accessing the network and to access by human users to terminal devices.

Although the importance of access control is widely recognised, the practical application of security techniques to solving the problem is more limited. This is for a variety of reasons including technical complexity, lack of agreed standards, lack of user acceptability and lack of supporting infrastructure (such as TTPs).

Secure access control relies on a mixture of:

- identification mechanisms (authentic naming) identifying the remote person or system
- authorisation mechanisms, determining the authority of the remote person or system to carry out different types of actions
- random (unpredictable) components, affording protection against the re-use of once-valid access control messages under invalid circumstances (replay)
- cryptographic techniques to protect the above from modification, copying, etc.

Without some analysis of access control scenarios, followed by some outline standardisation work, users and systems are going to find themselves having to implement and use (depending on their current application) a range of incompatible techniques, which in turn rely on only partially interoperable infrastructures (such as naming and identification authorities, certification authorities, key management systems, directory services, etc.).

Requirements

There is a need for widely accepted solutions to the most common access control scenarios. There is a need to:

- identify and group access control scenarios, to determine levels of commonality
- identify techniques, products, specifications and standards addressing access control, and associate them with the identified scenarios

- identify parameters common to most or all of the above techniques, products, specifications and standards and investigate the feasibility of establishing common formats for them
- identify the key features for coherence in the supporting infrastructure
- define a limited number of basic access control mechanisms for pilot implementation.

5.8.2 The individual right to signature

Issue

Individuals have the right to sign any information.

Discussion

Like with hand-written signatures, anybody is entitled to use a digital signature. Therefore, the distribution of keys for the purpose of signature must be non-discriminatory and non-restrictive. Separate from the signature is the question of authority, ie if a certain person is entitled to sign a certain element of information, document or transaction.

Signature verification is therefore a two step process: formal verification of the signature and verification of the authority of the sender. This process is depicted below.

It is assumed in this simple model, that the sender adds his certificate (name plus his public key) to the signed document. The formal verification then establishes that a person with a certain name has correctly applied his signature and that the document has not been modified in transfer. Verification of authority checks that the name has the legal authority to sign a particular document.

Note that as a consequence, the authority given to a person should not be included in the attributes of the certificate, otherwise any change in authority would invalidate the certificate.

The situation maybe further complicated by the fact that several signatures maybe required for certain documents, eg husband and wife plus notary, two company directors.

Requirements

- Clarification of the right to signature and the attached authority.

5.8.3 Consistency of legal principles

Issue

The legal functions have to be clearly identified for the authority of digital signatures, before a code-of-practice can be developed and introduced.

Discussion

In legal practice security and functional requirements for hand-written signatures differ widely. In some cases a hand-written signature is only to indicate that the signer has concluded his train of thought or his expression of will; under the given circumstances its authenticity may be obvious and need not be provable. In other cases, for evidence, the signature must be provably authentic. In yet other cases authenticity requirements may demand attestation or even ask for more than one person's signature or for public notification.

The spectrum of legal requirements can be matched by the spectrum of technical realisations which may differ with respect to security provisions just as widely as legal requirements. Yet the signing process must be transparent to the signer. For this reason it must follow standardised rules; specific man-machine interfaces must be familiar to the signer; i.e. they must follow a standardised layout principle.

For ease of transition (in judicial thinking) from hand-written to digital signatures traditional functional requirements for hand-written signatures should be met by the technical implementation of digital signatures as closely as possible.

A particular problem is the validity period of a digital signature. One must distinguish the validity period of the signature itself and the validity period of the authorisation.

The validity period of the digital signature itself may have to be limited for technical reasons. These reasons include:

1. Insufficient key length. One may discover that some years from now, new progress in mathematics and technology makes it plausible that keys of the originally chosen limited length can be broken. (For instance, several European banks have introduced remote banking with RSA keys of length 512 bits. One cannot guarantee that this will be safe in 10 years, or even less, from now.)

2. Poor key generation. One cannot be sure that programs at the desired quality level will be used by all key management centres. Hence users of those key management centres may find that their keys are breakable, and they have to cancel their certificates.

3. Weak protection of workstation. The secret key of a user may be compromised accidentally or through negligence. It may also be possible to tap the password of a user through a Trojan horse on his PC and subsequently get access to the secret key. (Fraudulent users may even claim this happened, and give away their key on purpose, in order to dispute that a certain signature did originate from them.)

Taking the necessary precautions, and taking a differentiated approach to the validity period of signatures, then most digital signatures would fall inside the scope of applicability of hand written signatures

The authority attached to a signature normally changes much faster. The authority given to a person should therefore not be included in the attributes of the certificate, otherwise any change in authority would invalidate the certificate.

However, in all the work that has been carried out so far, there is no solution offered to the following problem: If messages have been signed with a key and needs to be kept for a number of years, and that key is denounced by the user as being compromised, how can the value of the already calculated signature be left intact? One possibility might be to use a TTP for time stamping, but further study into this problem seems in place. An example may illustrate this point.

If a user A signs a message in 1993, which has legal consequences to user B until 2003, and A then cancels his certificate in year 1995, claiming that his key has been compromised, he will probably claim that the signed document from 1993 was falsified in 1995 by B, who could have bought a copy of A's secret key. However, if B upon receipt in 1993 had gone to a TTP and had the signature of A time stamped and signed by the TTP, or even registered, he can prove that A in fact did produce the said signature back in 1993.

For some sectors and/or applications the granularity of the time stamping will be critical. It is conceivable that trusted time down to one second accuracy will be needed.

Requirements

- The legal functions of signatures need to be agreed EC-wide/internationally. Once this is achieved, it is possible to determine to what extent a code-of- practice will suffice. One issue to be addressed is the intended use of the digital signature, and the legal responsibility and liability of the signing entity with regard to the signed information.
- Clarification of the conditions of acceptance of the authority of an digital signature, eg for legally binding purposes, ie as substitute for hand-written original signatures.
- Recommendation for the implementation for a public digital signature scheme for use by business, administrations and the general public.
- Legislative rules and, where appropriate, liabilities, for keys, certificates and TTPs need to be developed to cover revocation of any or all the entities involved in the "chain of proof" needed in the signature technique.

5.8.4 Signature schemes

Issue

Introduction of an international digital signature and identification schemes.

Discussion

Open communication requires standardised publicly available algorithms. It is possible, however, to develop a scheme for digital signatures, to get laws, regulations or directives in place, to develop supporting profile standards and to develop fully implementable models for TTPs, without specifying in detail the underlying algorithms.

The characteristics required of a digital signature mechanism include that it

- is practically unbreakable
- has a sufficiently large key space, performance (time and space requirements for signing and verification), reasonable size of key, etc.
- includes key generation.

In order to allow for world-wide, unrestricted use of a digital signature scheme, the mechanism should not be usable for the concealment of message content.

The minimum requirement should include

- an estimate of error probability if probabilistic methods are used
- an estimate of probability of occurrence of weak keys (perhaps completely improbable)
- a guarantee of sufficiently high degree of uniform distribution.

In so-called identification schemes (for access control), which do require public key techniques rather than conventional schemes, practical zero-knowledge protocols must be developed and standardised that fit a corresponding digital signature standard.

Requirements

- Development of specifications and standards along the lines described above
- development of specifications and standards for application oriented integration
- development of a general application programming interface (API) for integration of security services which could be easily integrated into most application (This could as well include codes which explain the intention of the applied signature.)

- development of transaction-oriented multiple signature schemes
- solution to the specification, standardisation and licensing problem of cryptographic algorithms.

5.8.5 Key usage

Issue

Digital signatures imply the specification of a full set of procedures dealing with the three phases of key management - user enrolment, key and certification distribution, and operational maintenance (revocation, blacklist, destruction), which must be agreed and accepted.

Discussion

In order to apply security to any message or process, four logical layers are relevant:

1. Legal intentions and implications
2. The definition and identification of the relevant security service to be applied.
3. The underlying mechanisms.
4. The algorithm and protocols.

Without standardising or agreeing on the 4th layer, it will not be possible to communicate.

In order to adopt electronic versions of negotiable and quasi-negotiable documents, such as bills of lading, new security services have been identified to meet business requirements, in particular claim of ownership for exchange of values. This needs to go through a standardisation process.

But also for more " classical" services, the current standards do not reflect the granularity of eg non-repudiation needed by business requirements. ISO 7489-2 only addresses non-repudiation of origin and delivery (sometimes called receipt). However, one needs at least origin, submission, delivery and receipt, where submission and delivery would correspond to the services required when a registered letter is mailed.

For hand-written signatures , a person typically knows what he is signing, which is important for legal implications. This is not so easy to achieve with electronic data. In particular it must be clarified to what extent the system must indicate to the user what he is actually signing.

Requirements

- Develop standards and profiles as described above, especially the development of profile - or functional - standards to support CCITT X.509.

5.8.6 Universal acceptance

Issue

For digital signatures to become a full alternative to hand-written signature universal acceptance is required.

Discussion

All functions of the hand-written signature should also apply to digital signatures.

Where legal functions are carried out by digital signature, consensus with the legal profession is essential.

Requirements

- Development, together with the legal profession, of recommendations for the practical use of digital signatures as a full equivalent to hand-written signatures in legal transactions

- demonstration, through pilot projects, that digital signatures can be used as equivalent to hand-written signatures

- inclusion in the curriculum of relevant educational institutes (eg engineering, law and business schools) the use of digital signature.

5.8.7 Security of electronically stored information

Issue

As legally and commercially significant information is transferred and stored electronically, the implications of this on long-term (10's of years) secure storage and retrieval must be properly understood.

Discussion

Industry is moving increasingly towards electronic trading in all its aspects. Governments are encouraging the use of electronic communication of commercially and legally significant information. As a result, there is a need both to establish irrefutably the origin of, and the delivery of, such information and, particularly, that the information has been signed and stored in an unforgeable way. This unforgeable electronic signature must be trusted for at least 10's of years for some information, and the associated information must be retained in a secure manner that is capable of human interpretation at any time during that period. Any system proposed for electronic signature storage must be as secure and robust as that currently used for hand-written signatures.

Any such system must allow for not just technical evolution, but also social change and other factors (e.g. the continued existence of trusted public key directory centres, or the way businesses merge, change or collapse).It is not currently clear that the way this can be achieved is yet accepted legally, or the full implications are even properly understood

Requirements

- Build on the digital signature experience to consider the long-term implications of the unforgeable secure storage and retrieval of legally and commercially significant information, with access by any authorised person or organisation internationally.

5.9 Privacy enhancement issues

5.9.1 Perception of requirements for privacy enhancement

Issue

Confidentiality is, at times, essential for the good functioning of administrations, business and human relations.

Discussion

Business user of telecommunications and information systems cannot obtain full business benefit without confidentiality services being available. There is a clear need for confidentiality services in the exchange of information in the business as well as in the private use. Today the exchange of sensitive information requiring confidentiality is often done in non-electronic form because for electronic transmission "confidentiality" is either not available or its use not permitted. With the increasing demand for fast exchange of all kind of data, demand for "confidentiality" will become pressing.

Most business and private users of communication systems are aware of the conflict between their confidentiality requirements and national security issues which require the possibility to intercept the communication in a way regulated by national laws. They accept the national authorities ability for this interception provided there are adequate safeguards to prevent unauthorised interception even by government employees.

Expectations of confidentiality of electronic message services can currently not be met in the absence of international standards or internationally accepted methods. Uptake of these services by commercial users to support business processes will therefore have a natural limit, ie to those messages that someone usually writes on a postcard. Examples of commercially sensitive information includes pricing and bidding strategies, mergers and take-overs, or from a privacy point of view (transmission of personnel and medical data).

User needs for confidentiality

In analogy with confidentiality offered by existing physical mail and archiving services, ie envelopes, registration, courier services, etc., there is a need for confidentiality in the situation of electronic interchange and storage of data. Even more so because electronic data can much more easily be copied or disclosed in its usual form, eg only channel coding and formatting as the "envelope", than its physical counterpart.

At present certain unclassified but sensitive information on physical media such as paper, microfilm, or photograph, of business enterprises or medical centres are protected against unauthorised disclosure by physical and procedural methods.

Today the trend is towards more electronic communication and storage of data and hence there is a need for appropriate confidentiality services in an agreed or standardised form to be readily available for all users of electronic information systems.

Service provision

The extent to which confidentiality services are provided for a specific business or citizen could depend on a system of licenses or certificates.

A particular business might qualify for a confidentiality license depending on its internal procedures and activities. A general (minimum) level of confidentiality could be provided to all users.

It should be possible for certain user groups or businesses to use other confidential services (egproprietary) than the standard ones provided.

There are strong indications of emerging "bottom up" solutions for these needs (eg the Pretty Good Privacy offering on Internet, beginning 1993).

Other initiatives (eg the announcement of the "Clipper Chip", 16 April 1993) illustrate the growing awareness of governments of the needs of their citizens for confidentiality services.

bf Awareness

In general users of electronic data processing systems are not aware of the threats involved in using those systems. Only after they have noticed (the consequences of) an unwanted or unauthorised disclosure of their information will they start to think of the inherent vulnerability of the system they are using. In view of this one should try to create more security awareness. Users, service providers, operators and authorities should achieve a certain minimum level of awareness of the issues involved in using confidentiality services before embarking on their use.

Granularity (meeting differentiated needs)

Confidentiality services at different granularity and for different types of telecommunication services are needed. Based on his risk analysis the user can then decide which level of confidentiality he needs and then use the services which provides this required level.

Some users may want a range of services of different assurance levels (analogy of courier services, registered mail, ordinary mail). Some users may want visibility of assurances to different extents.

Impact of loss of information and Impact of theft of information

By its nature, actual risks and impacts of disclosure are hard to quantify. But the absence of a baseline of protection of confidentiality will undoubtedly have a negative impact on commercial (and other) usage of international electronic communications in a wide range of business processes.

Actors and roles

Individuals may have a number of roles in more than one organisation - these need defining or clarifying. Their "role" as a private citizen is an important case. The organisations that act as custodians of roles need to be classified also. These are essential ingredients for domain management.

Mutual confidence and TTPs

Users and mechanisms to ensure that they get assurance of compliance to agreed "rules of procedure" from their trading partners, or other private citizens, with whom they are interacting using confidentiality services. TTPs are one mechanism for achieving this, but other lower assurance, lower cost solutions may also need to be considered.

Requirements

- Proposal for a frameworks and architectures which are accepted as well by the business users as by the national security agencies and the service providers
- standards for services and service provision. Ensure that the confidentiality services are compatible with existing communication standards and practices where possible
- verification of practicability of proposed solutions through suitable pilot projects
- model contracts for confidentiality services
- awareness of sector actors of the potential losses due to the absence of confidentiality services.

5.9.2 The case for the provision of public confidentiality services

Issue

The provision of public confidentiality services have to reconcile the needs of the business sector and general public with the obligation of public authorities to provide adequate protection while at the same time maintaining its capability to fight organised crime, maintain public order and national security.

A well developed public confidentiality service would provide for the obligations in a transparent manner.

Discussion

Business operates increasingly in an international and open environment. The communications take place via private and public networks. Modern network management techniques use alternative routing depending on traffic conditions. This implies that the physical communication is under the control of a variety of intermediaries working under different regulatory and legal conditions for data protection and privacy, and therefore one must consider the network as inherently risky. This means that end-to-end protection is required. This applies also to the general public using international public telephone networks.

It is a fact that business and the general public have been addressing their needs with public domain solutions (published algorithms and freely available software). However, the approach is awkward and its utility therefore limited, since, for example, there is no public directory and he has to manage the keys himself. A public solutions open to all users requiring electronic signature and confidentiality would remove the need for the use of ad hoc solutions. It would also provide for a transparent solution to the need for legally authorised intercepts.

If a public confidentiality scheme is offered, organised crime could also subscribe to such a scheme, but as it would include provisions for legal intercept, it would hardly be attractive. One would expect that such users would continue to find their own solutions as will the classified domain.

An open and public service offering a credible level of confidentiality would therefore provide for the honest user, while not worsening the situation with respect to public order or national security.

The combination of international communication and national security regulations require a common framework for confidentiality services, which on the one hand interoperate within all Community Member States as well as with countries outside the Community which themselves may establish their confidentiality services. This requires either an overlay approach or gateways which link the different national or regional services. These gateways are only required where multinational agreements for co-operation on national security concerns is not yet established. In this case these gateways may provide at least an interim solution.

In order to fulfil its function and eliminate the need for "home-made" solutions, the public confidentiality service must be open to world-wide use and provide its service in a non-discriminatory way.

Confidentiality services should ensure that

- Users are protected and obtain assurance against non authorised interception and disclosure.
- The confidentiality service is of high (technical, procedural) quality and evaluated as such by all Member States.
- Authorised disclosure of the protected user information (undo the confidentiality service) is under certain well-defined circumstances possible, eg by secret-sharing.

With this approach, confidentiality mechanisms details (description) do not need to be published or disclosed to the public in general.

While the use must be largely unrestricted, the systems and sub-systems or equipment for the independent implementation of aforementioned confidentiality services can be made subject of export controls, eg export is possible if:

- The users comply with the rules of the exporting nation (end-user declaration) with respect to the disclosure mechanism.
- Multinational business users form EC countries with "central" organisations.
- Other countries on a bilateral agreement liaise with EC if they comply with the rules.

Export restrictions are, inter alia, based on the concern that cryptography may be used by hostile governments or other organisations for the concealment of subversive information. The same concern does not apply to the use of cryptography for integrity and authenticity enhancing service.

There are technical solutions to provide only integrity, integrity plus signature, and integrity, signature and confidentiality. Confidentiality enhancement is de facto only meaningful in communications with also the two other functions being provided.

The problem remains that organised crime and hostile governments are not restrained from adopting public domain solutions or from developing "home-made" mechanisms. Furthermore they are able to exploit legitimate users of systems and solutions to their own ends by use of "traditional" criminal mechanisms of bribery, blackmail or threats to personal safety. Legislation could discourage non-authorised use, but cannot be expected to prevent it, particularly in the case of organised crime. Restrictive legislation impacts the "law-abiding user" much stronger than others.

Choice versus interoperability

The users and service providers may feel the need to choose solutions to achieve the assurance levels they require. But interoperability will dictate a limited set of possible choices being available, and costs of service provision will also focus debate onto efficient solutions.

Advice and instruction / prohibition

This may vary from country to country, however certain minimum-rules will need to be adhered to between parties offering interworking public schemes which includes beyond simply usage also systems and sub-systems or equipment for the independent implementation of such confidentiality services

Requirements

- Choice of architecture that minimises service vulnerability (The confidentiality that users enjoy will depend upon the robustness of the service that is offered. This in turn will depend upon the robustness of the architectures available to perceived threats: key theft, masquerade, deliberate denial of service, inadequate disaster recovery are examples of threats the vulnerability to which may be different for alternate architectures.)
- framework for the provision of trans-domain confidentiality services (Mechanisms are needed that provide for a defined way to pass from one domain to another. This will require collective or multilateral agreements for interoperation.)
- guidelines for pan-European confidentiality service providers
- model contract for relationship between service providers across national boundaries
- assurance criteria for service providers and operators
- accreditation process for mutual recognition.

5.9.3 Interworking of autonomous confidentially services

Issue

Till such time that a universal service is being offered, interworking between autonomous confidentiality services is likely to be the normal situation because of the differentiated requirements. This implies the need for generally accepted rules for the relationship between these services.

Discussion

For quite a time the conflict between national security issues and the business need for international communications has blocked significant progress in the area of confidentiality services in telecommunications. With the recent US initiatives, pressure from European companies will grow to have access to equivalent services. But within Europe we have the situation that neither the legal situation in the different EC countries nor their national security policies are harmonised enough to have a single confidentiality service scheme with a single algorithm established within the foreseeable future. Therefore it is necessary to have a framework, which enables user-transparent interoperability between different national or regional schemes and which do not block the way for a single scheme which may be established in the far future. Interoperability is also required with non-European schemes like the US. scheme. To provide this interoperability the way information is passed from one national security domain to

another has to be specified and the national schemes have to be compatible with this specified way. The establishment of such a framework for interoperability is therefore a subject which needs international harmonisation. Aspects related to this are requirements for the cryptographic algorithms and for key management issues.

Requirements

- Definition of minimum requirements to ensure interoperability, including standards, specifications, rules of procedure and operating practices
- demonstration of trans-European confidentiality services using a suitable application , eg the realisation of administrative telematics applications.

5.10 Motivation to acquire evaluated solutions

Issue

The advantage of the use of evaluated/certified solutions is not generally accepted for commercial applications.

Discussion

Formal security evaluations have been carried out at a national level by a comprehensive, costly and time consuming process. The investment in the evaluation process by the vendor has resulted in higher prices for the resulting secure IT product. The duration of the evaluation process, has resulted in many secure products falling behind the technical state of the art.

Up to now, this has detracted from their broader relevance in the commercial market. Users have often preferred lower cost, more functionality rich products unless forced to purchase evaluated and certified products through some public procurement policy.

Vendors, historically, had products evaluated separately by each national market and their supporting criteria. The resulting limited revenue opportunity did not justify the high cost of getting products evaluated.

It is necessary to change this view by convincing users of the advantages of purchasing evaluated/certified solutions. Rapid adoption of Common evaluation and certification criteria is essential to reduce cost and speed-up mutual recognition of the resulting certificates.

Requirements

- Rapid adoption of common criteria
- rapid agreement on common evaluation method
- portability of test results and mutual recognition
- work sharing between vendors, test centres and users to speed up the evaluation process
- establishment of the "value-added" for the use by administrations and business, eg in terms of liability protection
- consistent use in public procurement.

5.11 Consistency of procurement practices

Issue

National procurement guidelines for the purchase of evaluated/non-evaluated products are not consistent throughout the EC, nor is there a general agreement on when there is an obligation to use evaluated products, and when it is recommended but discretional.

Discussion

Some security evaluated IT and communications products are purchased as a result of a risk analysis where it is determined that the evaluated communications product better suits the organisation's security needs than a non-evaluated product.

However, a survey conducted of over 200 organisations indicated that, to a large extent, evaluated products are purchased today by organisations in the EC because of the expectation they will be required by law to use certified products. This type of legislated market is occurring especially in those Member States that were involved in the development of ITSEC.

Unless common procurement policies are established in the EC, the IT market will become a patchwork of evaluated and unevaluated products. This may create new barriers to the efficient flow of information.

Requirements

- Identification of categories of application for evaluated solutions
- alignment of national procurement policies concerning evaluated products
- investigation of to assist those member states not involved in the early stages of ITSEC to develop and test procurement policies that are based on evaluated communications products.

5.12 Information Valuation

Issue:

For insurance purposes and for tort law cases a common means of valuation of information and information processing resources is needed.

Discussion:

In the case of information processing resources, the valuation may be as straightforward as estimating the replacement value of computers or the value of computer time in the case of denial of service (eg: through virus attacks or other penetration). However, in the case of destruction or theft of information, the problem is less straightforward.

Obviously, it is not possible to set a standard for the value of information, so what appears to be a potential solution is to establish standards for valuation.

Requirements

- Definition of the classes of information used and the types of damage that could be caused to the information owners
- definition of the rights and duties of information ownership
- development of guidance for owners of information as to the actions that they would have been expected to take to protect their assets and avoid negligence charges
- development of the methods and procedures that should be used to establish information value.

6 Supply related issues

6.1 Supply related Issues - Trusted Third Parties

6.1.1 Role of Trusted Third Parties

Issue

The public and generalised use of digital signature and of confidentiality services and the conformance with the needs of law enforcement implies the availability of Trusted Third Party (TTP) services to provide essential functions.

Discussion

TTPs will have to inter-communicate internationally and thus form a network of Trusted Third Parties , based on an international framework for their operation.

Trusted Third Party services can be considered as value-added communication services available to users wishing to enhance the trust of the services he uses. Therefore TTPs have to be able to offer value added with regard to availability, integrity, confidentiality and assurance. Although TTPs may be set up on a national basis within national law, they must be trusted internationally.

There are different types of functions which may all or in part be fulfilled by TTPs. The exact nature and extend to which these functions are provided by TTPs will be dictated by practical considerations and may vary considerably.

In general the TTPs operate on the basis of information provided by the user. Certification of information is carried out on the basis of evidence of correctness provided by the user or generated by the TTP itself, eg the keys.

The major services a TTP may offer include some or all of the following:

- Name assignment, ie the function of assigning individuals' and enterprises' unique names and addresses. Individuals may possess several different distinguished names, according to their role, eg as private citizen and as employee of a corporation.
- Certification, ie the function to validate that a name and address has certain credentials, eg a public key for signature.
- Key Management for signature, ie the generation, distribution, establishment, and administration of public and private keys.
- Key Management for confidentiality, ie the function to generate, distribute and administer keys used for confidential communications.

- Management Services for Names and Credentials, ie the function to establish, administer and make available registers with the names of individuals and their certified credentials.
- Legal services, ie functions usually performed by the legal profession, mostly concerned with non-repudiation.
- Guaranteed Date and Time Stamping, ie the function to provide exact date and time on request, to support non-repudiation.
- Management of Negotiable Document Transactions, ie unforgeable non-personalised tokens (eg electronic Bills of Lading, electronic shares).
- Storage of Electronic Information for clients with appropriate guarantees of confidentiality and integrity.

Common to Trusted Third Party service providers is that they have to be accredited and audited, and that they have to operate under the law of the country using common guidelines. The figure below provides an analysis of the different functions involved in the establishment and operation of TTPs.

The diagram identifies four functions in this process. The functions are:

- the provision of the required good practices, rules and regulations for the accreditation and operation of TTPs
- the accreditation, re-accreditation and audit of TTPs
- the TTP functions themselves
- the use of communications and of the TTP.

This diagram does not imply any particular allocation of responsibility for the functions indicated.

The information flow contains the following major elements:

- National Laws. The operation of TTPs will take place within the laws of the country in which they are located. It is conceivable that some legislation has to be updated to allow TTPs to operate in an international environment.
- Good practices, rules and regulations for the accreditation, operation and audit of TTPs.
- Standards for communications.
- Good practices, regulations and laws for the use of communication services.

6.1.2 Operating principles of TTP

Issue

The need for common operating principles for TTPs.

Discussion

To be effective, TTPs must:

- operate securely
- operate within a consistent legal framework across the Community
- offer a range of services, with a defined minimum
- conform to European or international standards, where available
- follow accepted good practice
- allow for independent arbitration, without compromising security
- be monitored by a supervisory board
- be independent in its operation within accreditation rules
- have a public policy on service refusals, if applicable
- assume responsibility of liability within defined limits for availability and quality of service.

The key questions include:

- Has the TTP a contractual obligation of results in terms of availability, integrity and confidentiality?
- How and by whom are the loss and penalty determined in cases of fraud, negligence or failure of the TTP?
- What assurance to the final user is offered by the accreditation of the TTP?

Requirements

- Harmonised legislation to provide an appropriate framework for arbitration, supervision and litigation

- model for TTPs meeting the requirements of users and authorities.
- baseline for accepted good practice including a study of the level of availability, privacy and security required for the TTP by the final users and how much they are ready to pay for it
- definition of quality of service, including availability, confidentiality, response-time, rules of disclosure to law enforcement agencies
- operational guidelines, including descriptions of minimum set of services and standards to conform to
- standard clauses for the contract between the TTP and the user, concerning the liability of the TTP.

6.1.3 Accreditation and audit of TTPs

Issue

The need for harmonised procedures for the accreditation and audit of TTPs.

Discussion

Although the accreditation and audit of TTPs may be a local or national responsibility, the procedures to be followed must be harmonised and have a common basis in order to ensure mutual trust.

It is assumed that national governments will be responsible for approving accrediting bodies. This may require to create new national laws or to adapt existing laws.

From the TTP point of view, timely and fair responses to requests for accreditation will be important.

From the user point of view, the agreed terms of the accreditation need to be properly documented and inspectable.

To maintain public trust in TTPs, an audit process must be put in place.

Other issues are related to the

- requests for accreditation from service providers in other EC and non-EC countries
- certification of certificates
- authority and accreditor signatures.

Existing Community rules for accreditation (eg of test centers) should be used as a basis for this work.

Requirements

- Development of international guidelines for the accreditation and audit of TTPs
- adaptation of applicable legislation or regulations to provide an appropriate legal framework for use throughout the Community and in the relations with third countries.

6.1.4 Use of names and certification of credentials

Issue

Use of names and of credentials (eg the public key) in international communications.

Discussion

Name Assignment and Certifications Authorities are Trusted Third Parties. They have been defined and, to some degree, specified by CCITT X.509 "Directory - Authentication Framework". Their purpose is to allow for individual and authentic addressing of communication system users by means of their authenticated Distinguished Names. A user may ask a Naming Assignment Authority for a Distinguished Name. The Naming Authority will give him a Relative Distinguished Name and supplement it by its own Distinguished Name to the user's Distinguished Name. Thus, although a person may ask several Naming Authorities for the same Relative Distinguished Name, each of his Distinguished Names will be unique, because the Distinguished Names of the Naming Authorities, by definition, will be unique. The concept of an agent that handles the interfaces between the end-user and the naming authorities is important in providing a user friendly interface to this process.

The two functions of name assignment (or identification) and certification are "binding" operations. Name assignment binds a particular name to an entity (a person or device), and certification binds certain credentials to a name. The diagram below shows the double binding process.

A Distinguished Name and a unique cryptographic Public Key are made part of the user's Credentials. The Public Key can be used to verify a (ciphertext) signature which has been effected by the user's complementary Secret Key (not contained in the Credentials). Credentials are signed/certified by the Certification Authority. Thus the user's Certificate consists of the Credentials, their signature by the Certification Authority and, if necessary, the Certification Authority's own Certificate. The user is given his certificate, preferably in a tamper resistant chipcard.

After signing a message with his Secret Key the user concatenates his Certificate to the message and its signature. The receiver of the signed message can use the Certification

Authority's widely available Public Key to verify the signer's Certificate and Public Key. With the latter the authenticity and integrity of the message can be verified.

The security services related to name assignment and certification need further standardisation as well as legal recognition, both preferably on an international level.

The United States have already begun to apply relevant US national standards. Therefore, corresponding standardisation action should be started on a European level. Its results should be made the basis for a European contribution to international standardisation. At the same time an interface toward a legal usage of naming and certification services should be defined to ease the adaptation to and to provide for the compatibility of the various EC legal systems.

Other related issues are pseudonyms and anonymity, for which a business requirement has been identified. Different degrees of anonymity should be provided for according to the specific needs in digital cash, tele-shopping, registration in data bases for statistical purpose etc.

As described above, the ability to sign a piece of data is to be distinguished from the authority an entity possesses. This relationship is depicted below:

Requirements

- Development of guidelines covering the use of names, by specifying:
  - naming principles (hierarchy of naming authorities)
  - format of Distinguished Name/Relative Distinguished Name
  - requirements to meet by naming authorities
  - requirements to meet by the user
  - requirements for the protection of the name against changes
  - handling protocol between naming authorities, user and certification authority
  - change of names
  - recording of information pertinent to de-referencing of names (by the Directory).
- Development of guidelines covering the use of certificates, by specifying:
  - certificate semantics and format
  - certificate handling (production, issuance)
  - signature and its certification (method, process)
  - authentication of certificate owner (method, process)
  - expiry dates

- renewal of certificates (periodical)
- renewal of TTP public key (periodical)
- handling compromises of secret information (secret keys, PIN etc.)
- revocation of certificates and notification
- black listing and execution of certificates
- security requirements to meet by certification authorities.

6.1.5 Key management service

Issue

Key management services for signed and privacy enhanced communications between organisations and individuals.

Discussion

General

- Definition of responsibilities and obligations for services that provide trust in the integrity of communications and those that provide confidentiality.
- Development of codes of practice for the generation, distribution and storage and destruction of keys for both purposes (integrity and confidentiality) in environments that have varying levels of assurance.
- Definition of escrow services. Some of the secrets may be of paramount importance and may have to be distributed among trusted parties (distributed-secret-escrow agents) so that none of the parties know the complete secret and not less than a defined minimum of those trusted parties must contribute their part of the secret in order to produce the complete secret.
- Mechanisms and criteria for assessing applicants suitability for the use of TTP services. Not all potential users of TTPs may have the necessary attributes (eglegal status, financial viability, etc.). This essentially applies to TTP services for closed user groups.

Integrity and digital signatures

- Relationship between the key management functions, directory management and certification needs to be clarified.

- Timeliness of issuing signatures when an application is made - verification of "signature worthiness" of applicant - periodic review of "worthiness" of existing constituency of signature holders.

- Removal of signatures from "active list" and initiation of "attempted illegal use" audit. This is a "certificate management" - "key management" interface management issue.

Privacy Enhancement

- Management of the domain within which the confidentiality keys are valid. The identity of authorised subjects within the domain: Key distribution to those authorised subjects (people and automated processes.).

- Should the TTP define the domain as well as manage it: if not should another TTP hold the definition (ietable of authorised subjects).

- Assessment of the assurance level of the domain within which the confidentiality keys are to be used, ranging from vetted, cleared people with physical and logical access controls to un-cleared people in open environments.

Domains are an important concept in confidentiality provision. The following questions require an answer:

1. What is the scope of validity of a domain for certification and the scope of validity for a confidentiality mechanism? Who manages the domains? Who manages inter-domain issues? Does each domain need a different TTP?

2. Who determines the scope of a domain? Who is authorised to change it? (for both certification and confidentiality.) Is a domain a "contract", and under which circumstances?

3. What are the assurance criteria for domain management? Who audits a domain manager? Who maintains the principles of domain management as technology changes?

4. Should domains for certification and confidentiality be different in view of the fact that a confidentiality domain will be transitory and that therefore key management principles are different?

5. When should the use of escrow services be mandated to ensure domain integrity.

Requirements

- Single digital signature mechanism and specifications preferably consistent with other leading countries
- adoption of a confidentiality algorithm standard and specification, and a key distribution mechanism based on an asymmetric public key algorithm
- establishment of "domain assurance" levels and criteria for TTPs to use for confidentiality key management purposes
- codes of practice for TTPs engaged in key management activities, and the provision of escrow services and the methods by which those codes of practice would be audited
- set of criteria for mutual recognition between TTPs acting on behalf of organisations who wish to communicate securely. Merging of signature directories and secure inter-domain communications are fundamental issues.

6.1.6 Management Services for Names and Credentials

Issues

Whenever parties engage in bi- or multi-lateral electronic transactions, they need beforehand some non-transient information on their partners (such as identity, legal representatives or any other kind of credentials eg public keys). This does not imply permanent recording of such information.

Discussion

Management Services for Names and Credentials are established to facilitate access to this type of information, whereby service subscribers are provided with up-to-date data pertaining to the parties listed in there. Because partners may conclude the transactions on the basis of the information (at the minimum, the authenticated identity of their partners) they are provided with, and because some of the information stored by such a service may be protected by privacy legislation, the service itself must be trustworthy and the data it provides correct.

Management Services for Names and Credentials keep objects which are referred to by "Distinguished Names". A Distinguished Name is unique to a communication subject. A subject may have a number of (unique in the above sense) "Alias Names". It is required that the service can reference Alias Names to their subject's natural names. An Alias Name may be a pseudonym. Whether or not the service is allowed to reference a pseudonym and let inquirer know the result will depend on the subject's data privacy rights.

If, as is likely going to be the case, there is more than one provider and certifier of information, the Management Services for Names and Credentials must be part of a network of information suppliers. Network can be organised according to either geographical distribution or business sector or information taxonomy or all three of them. Users may have to subscribe to more than one such service or service type (eg "Public Key directory for the banking sector"). Users may have a number of different roles in an enterprise, each of which needs access to a set of different services. In the case of a multiple service and network of providers, one can speak of a system of Management Services for Names and Credentials.

Because of the damages that could be caused by the distribution of false information, the Management Services for Names and Credentials must apply due care in its operations. In the case of proven negligence the service could be held liable if inaccurate information were provided. The creation, update and destruction (eg in the case of certificate revocation) of information is either mandatory or forbidden. In critical cases (eg; certificate revocation), the update may have to be notified to subscribers without request.

The management of the Management Services for Names and Credentials must thus be accountable. There must be legislation, rules and regulations governing it.

Obviously, the service must cover and be available on an international level.

Obviously there is the issue of standardisation of the service at the user end (external interface) and between service providers (internal interface).

Since international Management Services for Names and Credentials are akin to internationally distributed data bases, they face the same legal questions: who is legally responsible for the information (between the creator, the storer, the distributor)?

Market pressures are bound to promote the advent of sectorial Management Services for Names and Credentials, and possibly their subsequent interconnection or integration into larger network. In order to avoid fragmentation among proprietary services, there may be a need to lay down base rules for naming, binding, certificates and the associated IPR rules.

Requirements

The basic issue is the provision of efficient Management Services for Names and Credentials, supplying various types of information is a requirement that needs rapid and efficient satisfaction.

- Provision of Management Services for Names and Credentials, to include
  - Identity (cf. issues on name authentication and referencing of Alias Names)
  - Name information (to enable the correct forwarding of messages (eg static digital network or GSM communications)
  - Credentials such as public keys or any signature-verification data.
- Interoperability specifications and standards.

- Harmonisation of legislation , rules and regulations concerning Management Services for Names and Credentials, intra-Community and extra-Community.

6.1.7 Legal services

Issues

Legal TTP services are offered essentially to prevent disputes, or resolve them in a structured, efficient, accepted by all parties involved and non-controversial way.

Discussion

Prevention of disputes arises essentially from the very ability of legal services to assign responsibility and fault, should one occur.

- Thus, legal services must essentially be able to verify the application or non-application of rules and the evidence pertaining to them.
- Legal services may or may not generate the evidence itself. In other words the question is whether a third party offering a trusted service also arbitrates litigations pertaining to its principal service. For example, does a signature generation service also provides signature-verification services?

Two issues arise in this topic:

- What is the legal status of evidence generated by TTPs ? Does it imply liability? What is the legal status of decisions made par legal services when they are not judicial but private(and corollary, what are the rules of appeal)?
- If evidence is not generated by the arbiter, how is the evidence acquired and authenticated and how is responsibility assigned? One is faced with the general problems of TTPs : operating rules and legislation, standardisation, inter-operability and accreditation.

Requirements

In addition to the ones concerning operation legislation, standardisation, inter-operability and accreditation, Community actions specifically aimed at legal TTP services could focus on

- the harmonisation of legislation on the legal status of evidence generated by any TTPs and especially on the intra- and extra- community recognition thereof. This probably implies the settlement of the accreditation question

- the promotion of community-level information technology litigation services modelled after existing international bodies such as the International Chamber of Commerce

- Essentially focus on - and restrict actions to the problems created by the fastest-growing services based on Public Key cryptography, eg verification of signatures, certificates, etc.

6.1.8 Guaranteed date and time stamping

Issue

Guarantee of unambiguous date and time of submission and receipt.

Discussion

In electronic communications, a digital equivalent is required for the date and time stamp in the paper world. Such a time stamp must be issued by an organisation that is trusted. If time stamps are simply attached internally by the sender or receiver of a message, then, in case of litigation, it will be difficult to establish if these were erroneous or have been forged.

In direct communications, both parties may agree on a mutual time reference, but in store-and-forward type communications time stamping by a third party is particularly important .

Depending on sectoral differences, different granularities of time stamps may be needed. Some sectors may be content with the date, some with the nearest second.

The third party must be trusted by both parties, or at least the dispute resolution mechanism, for the correctness of the date and time supplied, but also for the confidentiality with which they handle the contents of the correspondence.

The time stamping schemes proposed so far are impractical, because they require the recording of the time stamp and the document (or at least its digest).

Requirements

- Development of an approach to date and time stamping for time-critical transactions and applications, including a range of granularities of timing.

- international harmonisation of rules and services for time stamping, with the objective of achieving general recognition and acceptance of time stamps and their provision by suitably accredited service providers.

- international harmonisation of rules and services for time stamping, with the objective to achieve general recognition and acceptance of time stamps issued from different service providers.

6.1.9 Negotiable document transaction

Issue

Some conventional physical documents, such as eg the bill of lading and the bill of exchange, must be negotiable. The possession of the document must allow to give title to anybody who can present it. The electronic equivalent is also needed.

Discussion

Negotiable documents entail that their physical uniqueness must be protected against duplication; it must be easy to distinguish a copy from its original. This is the case with hand signed paper documents; the hand-written signature cannot be copied such that the copy could not be distinguished from the original. True, a digital signature does protect the integrity of the signed electronic document; however, it can be easily copied so that the physical original cannot be discerned from its copies.

This impedes the usage of electronic communication eg in maritime trade. The sender of a cargo produces a unique document, the bill of lading, hands a copy to the shipper and sends the protected original to the receiver. The receiver may trade the original and its title or keep it. Whoever presents the original to the shipper will be handed over the cargo.

The shortcoming of the paper bill of lading is the fact that it takes time to transport it, particularly as it is a piece of value and must be well protected. Therefore, an electronic substitute should be found that protects its originality and can be transacted in telecommunication systems.

The Document originality can be provided by the use of chipcards. A chipcard can store a secret and protect it. The secret is essential to authenticate the signature of the document. As the chipcard cannot be explored, the secret cannot be transacted into another chipcard. Thus it is practically impossible to duplicate the original chipcard. Such a chipcard can be made a substitute of the negotiable paper document.

In order to produce and to transact chipcard documents via telecommunication trusted equipment is needed. It Should be operated by trusted third parties, eg by public notaries. They may be bestowed with the responsibility to produce chipcard documents and to transact and receive them by means of their trusted equipment. Transaction may be performed by depleting the original chipcard at the sending end, securely transmitting its information and feeding it into another chipcard at the receiving end. This process must be protected for its integrity and confidentiality. Not even the "public notary" must be in a position to alter the information.

Beside issuing negotiable documents there are other ways of securing correct title to property. Instead of a person proving his claim by the presence of a token, the claim may be addressed to a distinct person who then is expected to prove his identity.

This - continuing with the above example - is the case with the freight bill, which is another way to deliver a cargo to the authentic receiver. However, the freight bill cannot be traded as effectively as the bill of lading, although, by omission of additional chipcards and other trusted equipment, it makes it easier to design the electronic substitute process.

One should expect that, unless proper electronic documents will be available, the use of paper for negotiable documents will be continued at the expense of effectivity and more paper.

Requirements

- Development of techniques for the establishment, handling and recording of Electronic Negotiable Documents.

6.2 Supply related issues - Evaluation of trusted solutions

6.2.1 Perceived Requirements for trusted solutions

Issue

Need of users for trusted components, products, systems, services and applications

Discussion

The trustworthiness of a given information system and its use imply an evaluation process. Depending on the needs of the customer, either vendor declarations or formal certification procedures may be needed. The choice of either of these mechanisms will depend, inter alia, on costs and delays involved in formal certification processes. A major factor is also the recognition of certificates in other markets and their utility, eg in protecting the user or vendor against liability claims, where it is possible to do so. In the safety related area, the trustworthiness of the development process and its execution are also critical factors and need not only evaluation but also auditing. The qualifications and experience of project managers and safety auditors are also factors which affect the resultant level of trust in the system.

Requirements

- International agreement on criteria and evaluation methods, and mutual recognition of test results
- clarification of the commercial value of “certified products”, eg in terms of liability limitation

- clarification of the status and implied liability of vendor declarations
- development of principles for liability definitions for multi-level, distributed services
- international agreement on the methods for evaluating safety critical system development processes, and the qualifications and experience needed for individuals to become managers and auditors of such activities.

6.2.2 International harmonisation and mutual recognition

Issue

At the moment different evaluation criteria and evaluation schemes are in use. These are especially the US, TCSEC, the European ITSEC and the Canadian CTCPEC. Other countries like Japan have first drafts of criteria. This situation is not acceptable to international manufacturers who would have to perform different evaluations against different criteria and schemes for a single product. This will unnecessarily increase the cost of the product without enhancing the security features.

Discussion

Different activities have already been taken or are currently on the way to harmonise evaluation criteria and evaluation schemes. The ITSEC and ITSEM are a result of such a harmonisation process within Europe, and the United Kingdom, France, Germany and the Netherlands are discussing the mutual recognition of each other's certificates based on ITSEC and ITSEM, with the intention of achieving agreement in 1994.

In North America, the US and Canada co-operated in the production of the first draft of the Federal Criteria. Following publication of the Federal Criteria in early 1993, it has been decided to make all effort to align the ITSEC and the Federal Criteria to produce a joint European/North American set of Criteria compatible with existing practices in both North America and Europe in 1994. This is the first step towards international harmonisation between the two groups.

Based on these activities, ISO/IEC JTC1/SC27, Working Group 3 is working on an ISO standard for evaluation criteria.

But harmonisation of the criteria is only the first step to reach mutual recognition of evaluation results. It will need to be accompanied by agreement on methodology, schemes and certification bodies. Only then will mutual recognition between North America and Europe be possible.

Even within the European Community mutual recognition has turned out to be an arduous task and mutual recognition of certificates is not yet achieved, mainly for legal reasons. This indicates that world-wide mutual recognition of certificates requires many, yet unknown, problems to be solved.

Some activities for international harmonisation of evaluation criteria and evaluation processes are currently in progress but only one result of such a process which seems to be stable and widely accepted has until now been achieved. This is the ITSEC. But even in Europe the subject of harmonising the evaluation process turns out to take much more time than the harmonisation of the criteria. The reason for this is that the ITSEC could be adopted by different countries quite easily without significant changes to their existing evaluation processes (and almost no changes to the certification schemes). The real changes to the established practices come up when you try to harmonise these two topics, since this results in significant changes to evaluation and certification practices and may even have legal consequences.

Looking into the international arena, the only evaluation process and certification scheme in the area of communications-security which is in place for a significant time is (beside the European one) the US TCSEC evaluation scheme. But the focus of this scheme is mainly to evaluate and certify commercial operating system products suitable for government applications. Currently the US are trying to widen this scope with the Federal Criteria and the accompanying trust technology programme of NIST whose main goal is to establish a more commercially oriented evaluation and certification scheme with industrial evaluation facilities like the ITSEF's in Europe. Both the Federal Criteria as well as the trust technology program look like a much better basis for international harmonisation but nevertheless a considerable amount of work is necessary to achieve this goal. But since both the new criteria as well as the commercial evaluation process are not yet established in the US there is an opportunity to influence this process. The fact that the US sponsors two parallel ITSEC evaluation of their TMach operating system show clearly that the US side watches the European activities in this area very carefully and tries to get as much information as possible (both positive and negative!) about the European evaluation process.

Even for the old TCSEC evaluation scheme the US showed great interest in comparing this scheme with the European ones. Joint tasks between the CEC and the US side represented by NIST and NSA material about the various evaluation processes was presented. This shows a will for co-operation which is clearly based on the fact that US manufacturers sell more communications-products in Europe than vice versa. Other countries like Sweden, Australia and Japan watch this process very carefully.

Requirements

- Establishment of conditions and procedures for mutual recognition of evaluations
- establishment of conditions and procedures for EC-wide/international evaluations
- international and EC standardisation of evaluation criteria and methods.

6.2.3 Vendor declarations

Issue

For applications that need security, but not the kind requiring formal evaluations, vendor declarations are used. These are, however, at present not defined in terms of what they cover and what assurance they offer compared to formal evaluation.

Discussion

Between the requirements of governments for formally evaluated solutions and no evaluation at all, there is a large part of applications used by business and the general public. Vendors do address security and provide some level of assurance, but its significance, particularly in an open environment is not obvious.

Requirements

- Development of an agreed definition of scope and liabilities of vendor declarations for secure solutions.

6.2.4 Evaluation of applications

Issue

The user interest is finally with the security of his application. The use of secure products and services is a necessary but not a sufficient condition to meet the user requirements for the protection of the application.

Discussion

At present, evaluations and certification schemes address primarily products and systems. Communication services are only partially addressed and applications running on the products and via networks (in particular public networks) are left to the user to address. However with the restrictive handling of confidentiality mechanisms and opposition against end-to-end encryption, the user is left exposed.

Requirements

- Extension of ITSEC criteria and methods to cover services and applications.

6.2.5 Evaluation of communication services

Issue

With the ITSEC and ITSEM Europe has already a scheme for the independent security evaluation of IT-products and (to some extent) IT-systems. At the moment this scheme does not fully cover the aspect of the evaluation of telecommunication services, but extensions to this scheme seem possible which are able to address the items not yet covered by the current ITSEC/ITSEM scheme.

Discussion

The main item where communications security is considered in the public is in the area of telecommunication services. Especially when people send sensitive information to others using telecommunication services they are interested that this information

- gets to the intended recipient(s) in time
- is not altered by the service
- it not received by anyone else than to the intended recipient(s).

Not all these aspects are of the same importance for each kind of communication. The level of importance is highly dependent on the kind of information one wants to transfer.

The use of telecommunication services grows rapidly as more powerful equipment and services become available. A lot of companies and especially administrations have policies which forbid the use of specific telecommunication services for highly sensitive information since they do not trust the communication services providers that some of the above mentioned security issues are enforced adequately. They use conventional techniques for the exchange of sensitive information with conventional security measures (eg sending sealed letters by registered mail or by courier).

In a time where industrial success depends on the fast exchange of all types of information these conventional techniques become more and more unacceptable. So the service providers will incorporate security provisions within their services. But nevertheless a lot of companies (and the national governments) will continue to use the conventional techniques since they do not trust those security services unless they are under their own control or being verified by independent experts.

Providing a security service as part of a telecommunication service will normally result in all entities involved in the provision of the telecommunication service being involved in providing the security service. Additional entities may even be necessary (like eg a trusted third party for key management issues or authentication services). These entities use systems and products to provide their part of telecommunication (and security) service. The total service is therefore provided by an interaction of all the entities.

The current ITSEC/ITSEM scheme is aimed at the technical evaluation of security measures within products and systems. It does not cover organisational, personnel, administrative or non-IT related physical security measures. Still many security services for telecommunication will heavily rely not only on IT-security measures but also on the above mentioned other security controls. For example a trusted third party will surely need extensive organisational, personnel and non-IT physical control. So it is clear that an extension to the ITSEC/ITSEM evaluation scheme is necessary to cover these aspects. The following section tries to identify how this can be done and which areas are not yet covered.

Looking at communication services one can easily identify several different types of communications-products and systems which have to co-operate to provide the service. This includes for example

- the end user equipment (telephone, modem or even his computer)
- digital dialling switches
- data concentrators
- conventional computer systems with databases for eg user profiles, directory information
- conventional computer systems providing mailbox services
- the communication media
- gateways etc.

For a specific telecommunication service one can identify the task each of these products or systems has to fulfil to provide this service. The same is true for security services. Each component involved contributes for one aspect of the security objectives or functions. These will then differ significantly in the functionality as well as in the assurance level required. Various topics regarding this may lead to problems, for instance:. assumptions on the security provisions to be taken in the environment of the product or system. Some of the security measures will heavily depend on hardware features. Evaluation of non-IT security features, like effectiveness of personnel and administrative security measures has to be established. The integration of all security measures has to be checked for consistency, completeness and effectiveness. For the evaluation of a communication service, therefore, different evaluations of systems involved in providing the service are necessary before the whole service can be evaluated.

Requirements

- Extension of ITSEC to cover more explicitly evaluation of hardware security features
- establishment of a formal accreditation scheme for secure communication services
- development of accreditation guidelines for the telecommunication sector

- trial service evaluations for existing telecommunication services
- articulation of the requirements of service evaluation.

6.2.6 Trusted network management

Issue

Trusted Network Management systems need to maintain a given assurance level while optimising the use of communication assets to achieve good economics and quality of service.

Discussion

There is a growing dependence in the security of network management systems for managing and controlling the provision of telecommunications. This is due to an increased reliance on distributed systems, the provision of new value added services and operations, and on the increased sophistication and richness of network and service functionality. Such dependency is placing greater demands on performance and quality of service. Tomorrow's electronic highways should be managed networks that should ideally interoperate in a seamless way to ensure efficient "self-healing" network operations and flexible creation and provision of a broad range of services, including those supplied by third party suppliers. The management of telecommunications systems security is thus growing in complexity commensurate with the growth in communications systems and the associated services and business use.

The major network management issues involve the protection of electronic information in storage, in transmission and being processed. Information used and applied to the controlling and maintenance of networks and services. Information that is used as input to the process of decision making and operational support, and which is also used as input to the emerging new wave of intelligent systems and communications. The provision of appropriate and effective network management solutions is fundamental to the success of the future telecommunications infrastructure for Europe.

Given the complex telecommunication systems that are evolving, the interrelationships that are needed for multi-domain working, grade of service requirements against a future European framework for legislation and regulation needed to maintain multi-domain working, the provision and maintenance of network management security the question of security evaluation is a key issue. What is the alternative if evaluation of network management security is not carried out ?

There are a number of constraints imposed by end users, service providers and network operators on the provision of security for network management eg concerning the employment of intelligence in networks and the idea of securing shared resources, dealing with different threat analysis and the responsibility for service liability.

Requirements

- Methods for network management evaluation
- extension of ITSEC to cover the evaluation of network management systems
- definition of Functionality Classes (or Protection Profiles) suitable for systems, products and services used in network management systems
- accreditation guidelines for the trusted network management
- trial evaluations for existing network management systems.

6.2.7 Modifications to evaluated products and re-evaluation

Issue

The shortening life cycle of products and the rapid evolution of services and applications due to competitive pressures implies the need for frequent adaptations and therefore re-evaluation.

Discussion

The impact of Open System, with its emphasis on portability and interoperablity, has resulted in many new products being incremental releases of existing products, for new operational platforms, applications, etc. There may be multiple releases or versions of a hardware or software solution in a short period of time. The maintenance issues of many similar and homogeneous configurations making up a product line is being understood.

The evaluation and certification of the product may take longer than the period between releases or updates to the solution. A certificate currently applies to a specific release or version. Changes may invalidate the certificate.

There is a need to devise a method to cope with these product or system changes so that the certified status of a product may be maintained.

Particular concerns include:

- Scope of the evaluation - Is an evaluation necessary for every single platform-dependent configuration of a product already certified?
- Assurance - Is it necessary to have an entire new release evaluated again in which only a small modification occurred (eg a spelling mistake in the user interface)?
- Re-use of previous evaluation work and results - Must the evaluation of sensitive and relevant but unmodified components of a product be repeated?

ITSEC and ITSEM have created a good basis on which to identify the key issues of re-evaluation and subsequent re-certification.

Practical experience of re-evaluation is limited but the problem may be mitigated by identifying key requirements. One approach is to categorise code in the security Target of Evaluation (ITSEC-TOE). This "Traffic Light" approach includes:

1. GREEN code that has no bearing on the security functionality of the product or system and that may be modified in future releases without impact on the security of the product or system.
2. YELLOW code that might impact the security of the product or system and that must be inspected by an independent party (such as an INSEF) before re-certification can be considered.
3. RED code that is critical to the security functionality of the product or system for which may modifications may require re-evaluation of the whole product or system.

This structure will assist developers, evaluators and certifiers in containing the level of necessary re-evaluation commitment following any modifications.

Experience is available on the parallel field of quality evaluation of software products. A framework for re-evaluation is outlined in ISO9126 and associated processes. It is likely that the impact of software quality on "operational" correctness of security products will force alignment of the various processes.

Requirements

- Effective feedback from existing Community schemes, both national and ITSEC related, on the problem of re-evaluation
- product-line structuring, understanding the current strategic development of IT products and how this is likely to change product cycles
- closer harmonisation of the evaluation process of all system and product "qualities" (performance, reliability, security) and how these may re-enforce each other in any re-evaluation actions
- development of criteria for re-evaluation decisions
- development of "critical event" approach to re-evaluation
- development of self-diagnostic techniques and procedures for IS maintenance.

6.2.8 Performance reporting for trusted products

Issue

Obligation to take corrective action in the case of faults found in evaluated products.

Discussion

Despite the successful evaluation and certification of a product or system, there is a small chance, smaller with the higher assurance levels, that a security related fault will be detected. The Developer is likely to have this fault reported to him and ought to take steps to correct this fault as quickly as possible and issue a new release of the software or hardware. The Certification Body needs to be informed of the fault and the steps the Developer intends to take to correct the fault. The Certification Body and the Developer need to discuss the need for any re-evaluation work and agree a timescale for this. Where a Developer is unwilling to correct the fault, the Certification Body needs to decide whether to withdraw the certified status and publish the fact that a fault exists, although not necessarily the details of the fault.

Requirements

- Incident reporting system for Certification Bodies
- definition of user and supplier obligations to report incidents.

6.2.9 Rationalisation of evaluations

Issue

Speeding up and lowering cost of evaluation and thereby improve attractiveness of security evaluations.

Discussion

Two key factors to the success of a security market enhancement are that evaluations are approachable and that the products or systems are developed in a way that is meant to meet the ITSEC requirements beforehand. It must also be understood that in many industrial cases, security, while indeed an important feature of a product or service, is only one aspect of an even larger target which is product quality or the quality of service.

Considerable work has been carried on in the broad field of software quality and its engineering which might be valuable to the security community.

Three standards address quality through an evaluation and certification approach, namely ISO 9000, SEI CMM and ISO 9126, at the organisation level, at the process level and at the product level, respectively. Those standards are well established and the demand for certificates based on them is growing rapidly.

There is an urgent need to consider the harmonisation of the ITSEC and ITSEM contents, to take into account to a much larger and clearer extent the benefits brought by those standards to security and to help reduce costs and needs of several, disconnected or even conflicting evaluations and certificates. The ITSEC approach seem to be sufficiently well accepted today to consider its integration into a broader context.

A closer technical look at quality standards and ITSEC/ITSEM taken together shows that, although they are all basically based on the same fundamental ideas and principles, there are residual conflicts when evaluations are to be carried out, either due to different requirements or to different evaluation approaches.

There are many ways in which the ITSEC could be turned more compatible with the quality certification domain. The following steps seem relevant:

- While preserving the current technical principles and requirements, a better distinction between specifically security related requirements and more quality related should be made so that it becomes clearer, if not explicit, what the various other evaluation systems and associated requirements can cover or contribute to.
- As all standards evolve, the ITSEC and ITSEM will have to be updated, at the level of the actual required deliverables for instance, to be directly compatible with what the other domains require, while still keeping its specificity.
- As the certification bodies of the quality fields become Trusted Third Parties for the ITSEC community, parts of the current ITSEC requirements might eventually be replaced by requirements for relevant quality certificates, and hopefully vice versa.

This plan suggests that the first step is one to consider directly today.

Few people involved today in security and its evaluation have a software quality background, which has impeded until now the harmonisation of the ITSEC with the other standards. Awareness raising actions on this topic should be considered with a fairly high priority level.

Requirements

- Alignment of security evaluation criteria and methods with those for quality and safety
- establishment of portability of results between quality of service, safety and security evaluations.

6.3 Supply related issues - technological change

Issue

Changes in the way in which technology is used throughout society will result in demands for new technological approaches to information security.

Discussion

Over the next decades it is to be expected that the macro economic climate will change dramatically. This is mainly driven by the shift in geographic location of the generation of the worlds GDP from North America and Europe to a more even spread, with the Pacific rim countries producing a larger share. The health and nutrition problems that will face the developing world will become more acute as a greater fraction of their population enters adulthood.

Information underpins these processes in a number of ways. The financial aspects of global businesses will become vital to their survival and the timely, accurate and where appropriate private communication of financial information on a global and adaptable scale will be critical. Health care information will need to be routinely available as health carers deal with the health problems of an increasing number of mobile people. Transportation of food to areas in need will require logistic information to be available in remote and underdeveloped parts of the world quickly and accurately.

The developed world will make increasing use of their less structured employment patterns to earn money in a variety of ways and in performing a range of tasks, less and less to do with manufacturing. Success will only be possible by the exploitation of mobility and wide bandwidth telecommunications services. It has the potential to provide quality of life together with high productivity. The effectiveness of this approach, in providing a method of revenue generation, will depend, inter alia, upon the performance, reliability and security of the information and transportation infrastructures.

Driving technologies within this scenario are:

- Wide bandwidth telecommunications, including
  - Multi media applications and communications
  - Global teleconferencing
- Mobile services for all applications
- Gigabyte storage in portable systems
- Robotically controlled transportation mechanisms.

It will be essential for a range of security and safety features to be embedded as a matter of design in all infrastructures, services and applications for them to deliver the benefits that are expected by their users.

Requirements

- Wide bandwidth telecommunications.

  Bandwidth will become a commodity on telecommunication systems. The added value in using it comes from the quality of service provided. One aspect of such quality is that of security. To provide security on wide band public switched networks, investment is needed that is focused on those aspects of security that are required by a) the telecoms service provider for his own purposes and b) the end user to support his application. Community wide and international specifications on security in ATM, SDH and associated signalling structures will be necessary.

- Multi media applications and communications

  Multi media applications will integrate all known representations of information into files, documents, messages and displays. Representations such as voice, audio, still image, text, video and graphics will become interchangeably available from a range of equipments that users interact with, including mobile telephones, personal computers, television sets and personal communicators. All aspects of security must be incorporated for potential implementation an all of these systems in order that a user may implement a level of security service appropriate to the application and the environment.

  A key issue is to maintain the "veracity" of the information transmitted. Veracity is the feature of a piece of information (eg a video sequence) to be true. Veracity is a wider concept than integrity which is only concerned with the protection of information during transmission and storage.

  Another issue is concerned with the protection of information through copyright. Without suitable technical means to safeguard the interests of the information owner, the evolution towards the information society will be seriously hampered.

- Global teleconferencing

  Teleconferencing is becoming the substitute for travel. In order to make it really cost effective all the above applications, multimedia, mobility, access to mass data and if necessary access to one or more parties who are travelling in private vehicles need to be incorporated within the teleconferencing application. True geographic independence will come only if such an application works on a global scale and provides all the security services that are needed by the community of users. Such an application will demand the integration of the security services provided for each of the sub-applications alone. Specifications to allow such integration should be defined and the technology to provide the security functionality developed.

- Mobile services for applications.

  Mobility provides the end user with geographic independence. The price paid for this independence is infrastrucural information and process that allows his demands on the infrastrucural services to be met wherever he is. Such information and process has to, by design, have security features incorporated. At the community level extensions of the GSM concepts to allow all applications to function securely in the way telephony does on GSM will require significant technological investment.

- Mass data storage and communications in portable systems.

  Access to huge amounts of data from a mobile terminal will be essential. Such data needs to be communicated securely, whether it be held in volatile memory, in the form of mechanically read ROM or transmitted over a network. Specifications for securing such data need to be developed as do the necessary bulk encryption services for huge data volumes . The technology components of such services will be a major challenge and need to be defined now.

- Robotically controlled transportation mechanisms.

  Human involvement in controlling mass transportation mechanisms is already decreasing as technology becomes more reliable. If human involvement for individual transportation is to shrink in the same way then mass production of cost effective safety assured technologies will be essential. Collision avoidance , guidance and navigation systems will be essential parts of every domestic vehicle and the requirements for the information safety and security critical elements of such systems need to be defined, standardised and developed .

7 Liability related issues (Consequences of Security and Safety Incidents)

7.1 Framework for international law relating to IS

tba

7.2 Legal provisions for liability in global services

Issue

Liability is a difficult issue under the best of conditions, but in the context of global telematics services it remains a matter of great concern but so far few advances have been accomplished.

Discussion

Liability is dealt with normally by a mixture of laws, regulations, conventions and counselling reinforced by risk sharing arrangements, in particular insurances. Legislation has so far evolved slowly and is still far from the point where it can deal effectively with the issues on a national level. When it comes to deal with liability under international law things become even more difficult. The same applies to regulations. It is only the insurance industry which has started to cover some of the risks. With the rapid increase in the use of telematics clearly there is a need to come to a better understanding of liability in the context of world-wide networking of services.

Requirements

Development of international framework for private law, especially liability

- Application of "Verursacherprinzip"

Under this kind of liability the source of the information has the responsibility to assure the proper use, its accuracy and the compliance with the law and regulations. In the case of intermediaries adding value the principle would be carried forward since the quality of the information may have been significantly changed.

- Application of "User Principle"

In this case the user is made liable for the what is done with the information and its consequences. He has to take all necessary steps to ensure that the information is correct and applicable to its use.

7.3 Insurance issues

Issue

tba

Discussion

For the public safety risks are addressed by the Insurance Industry with the premiums calculated on the basis of the assessment of risks reflecting past experience. For the risk associated with information systems there are only the beginning of an extension to cover this kind of risks. As the taking out of insurance policies is a natural, or partial alternative to IS measures, an improved methodology for the assessment of risks is important in adopting the most economic and practicable solution. Of course, there are some application areas where this approach is not or only partially acceptable.

Requirements

tba

7.4 Monitoring of compliance

tba

Development of framework for the monitoring of compliance to regulations, recommendations and good practices

7.5 Metrics for loss assessment

Issues

There is a fundamental need for guidance of any kind on how to access the loss and damages an organisation might face and how much of this might be addressed by evaluation and certification. Such metrics would increase the perception of the value of a formal evaluation scheme.

Discussion

Action is necessary to ensure the effective international exploitation of the security product evaluation and certification scheme. There must be a competitive business advantage of developing, implementing and using certified security products, and there must be a well understood correlation between a certified security product and the problems that it can solve.

Progress is hindered by lack of independent measures of the business relevance of the certified product.

Measures can be obtained by:

- vendor/user studies (from actual risk assessment)
- product comparisons (using loss reduction models)
- insurance contracts (both direct and consequential damage assessment)
- vendor cost/benefit profiles (market penetration, Software engineering costs, etc.).

Such studies would prove invaluable to the SMEs who cannot justify extensive Security controls yet are probably the most vulnerable to the consequences of information abuse.

The ITSEC actions should reflect a balance between the product based concepts of security objectives (codes of good practice) and quantitative risk/loss assessment.

This should result in measured, affordable controls as a prerequisite to developing a European and international security market.

Requirements.

Such a quantitative approach must address:

- mapping, certified product features to specific security incidents
- common, product independent risk analysis processes
- insurance processes recognising the advantages of certified products
- security incidents are the recognition by the legal, regulating and financial community.

A short term approach would be to raise awareness of the security exposures of using poorly complying (non-assurance, non-certified) products.

8 Spectrum of Measures

8.1 Common Framework and Consensus

Objective

To provide a minimum framework for trusted information and communications services on an international scale and to establish a multi actor consensus on essential requirements and options for the provision of information security and related issues.

Background

Information and its exchange via global networks is inextricably associated with all public and private activities involving the citizen, service providers, operators, vendors, administrations and authorities in numerous ways for all kind of purposes. With the increasing globalisation of the economies an agreed framework for the protection of information either associated with intellectual property, privacy, internal security and other legitimate reasons is needed. While there are several conventions and recommendations, the rapid evolution of technology and services implies the need to reflect on a common framework which could assist countries and regions to maintain interworking and avoid technical barriers to trade and communications without compromising their priorities in the protection of information assets.

Solutions for open communications between a variety of parties on a global scale do exist. They differ in detail and convenience in usage. However, the ability to use them depends critically on a broad consensus on the use of one or the other option. Nationally constrained solutions, such as DES, RSA in the USA are of little utility if they can not be used by US business in the pursuit of their global business interests and vice versa if others can not make use of these techniques for their communications with US partners.

To achieve agreement and reasonably general acceptance by the users concerned is as important as the technical performance of the solution in question.

Tasks

Development of a Common Framework to address the following issues:

- Revision of scope and approach to information security to reflect the new conditions, challenges and requirements brought about by globalisation (4.1.)
- Verification of the existing provisions with respect to their conformance to the Internal Market Policy of the EC implying the removal of existing internal barriers and the avoidance of the formation of new technical barriers due to divergent application of IS rules, regulations and legislation (4.2.)
- Definition of a common approach defining rights, responsibilities and duties of citizens and business on the one hand, and that of the authorities on the other hand (4.3.)
- Development of a common approach defining the rights of citizens and business users on the one hand and that of corporations, organisations and authorities using biometric techniques (4.4.)
- Development of a generic framework for the management of open and protected communications in a user/business oriented environment (4.5.)
- Concerted effort to address the common requirements of business, citizens and authorities to adequately protect non-classified information and its communication (4.6.)
- Common approach to the assignment of responsibility and liability (4.9.)
- Clarification of "Info-Ethics" for the professional and individual user in its relationship to Information Security
- Clarification of responsibilities of the sector actors in general and in their relations within each other, with particular reference to open and distributed applications (4.10.)
- Concerted effort to address a common approach to the handling of security and safety critical requirements (4.10.)
- Development of a common approach to security evaluation of information systems in safety-critical environments (4.11.)

- Common framework for domain interworking (5.6.)
- Clarification of the right to signature and the attached authority (5.8.2.)
- Common approach to the security of electronically stored information (5.8.7.)
- Proposal for a frameworks and architectures which are accepted as well by the business users as by the national security agencies and the service providers (5.9.1.)
- Framework for the provision of trans-domain confidentiality services . Mechanisms are needed that provide for a defined way to pass from one domain to another. This will require collective or multilateral agreements for interoperation (5.9.2.)
- Adoption of a confidentiality algorithm standard and specification, and a key distribution mechanism based on an asymmetric public key algorithm (6.1.5.)
- Develop an approach to date and time stamping for time-critical transactions and applications (6.1.8.)
- Establish conditions and procedures for mutual recognition of evaluations (6.2.2.)
- Development of an agreed definition of scope and liabilities of vendor declarations for secure solutions (6.2.3.)

8.2 Awareness, education and training

Objective

Improved awareness of the issues of information security by specific actions and a greater emphasis in the education and training of related professions.

Background

In the end it is the human factor which decides the level of information security, irrespective of the technical and operational measures one may wish to deploy. In this sense awareness and the teaching of appropriate skills in the context of the information professions, is an important measure to be considered. This may entail the creation of special training schemes and curricula, but most of all the appropriate inclusion of information security related issues in the teaching of information professions in general. This is in many cased essential, since information security is very closely related to the way information is used in a given context, ie often it has to be embedded in the application and management procedure and can not be added on as an external procedure.

Tasks

- Inclusion in the curriculum of relevant educational institutes (eg engineering, law and business schools) the use of digital signature (5.8.6.)

- Awareness of sector actors of the potential losses due to the absence of confidentiality services (5.9.1.)
- Initiate investigation to assist those member states not involved in the early stages of ITSEC to develop and test procurement policies that are based on evaluated communications products (5.11.)

8.3 Agreements

Objective

International agreements on a minimum set of features and operational concepts as required for trusted and open service provision.

Background

While a common framework and general consensus may go a long way, there is the need to get formal agreement on certain aspects. These may, for example, relate to issues surrounding liability, accreditation and certification and the fighting of organised crime..

Tasks

Development of a Common Framework to address the following issues:

4.4. Human Rights and biometrics

4.6. Management of Openness and Protection

4.7. Common concerns of commercial and national security

4.8. Security and Law enforcement on international scale

5.6. Security domains

5.8. Signature issues

5.8.2. The individual right to signature

5.8.3. Consistency of legal principles

5.10. Motivation to acquire evaluated products

5.11. Consistency of procurement practices

6.1.4. Use of names and certification of credentials

6.1.5. Key management service

6.1.6. Directory services

6.1.7. Legal services

6.1.8. Guaranteed date and time stamping

6.1.9. Negotiable document transaction

6.2.1. Perceived Requirements for trusted solutions

6.2.2. International harmonisation and mutual recognition

6.2.3. Vendor Declarations

6.2.4. Evaluation of applications

8.4 Common Practices and Codes of Conduct

Objectives

Development of Codes of Practice to

- support the development and harmonisation of sectorial practices
- support the development of a standardised approach to the development of baseline controls
- support the development and harmonisation of baseline controls.

Background

Codes of practice are found in many industries and disciplines. They encapsulate the collective wisdom and experience of the practitioners of a trade or profession or of an industry. For example codes of practice for the building trade. To the practitioners of a trade or profession, the need for codes of practice is self evident.

Codes of practice are not always obvious because they are often given other names. In some situations they may be called standards manuals in others requirements specifications. The property that sets them apart and makes them recognisable as codes of practice is the encapsulation of collective wisdom. The collective wisdom represents the means by which all parties to a transaction are protected from harm. In legal or business management terms this may be called a "standard of due care."

Any professional discipline needs to have a vehicle to encapsulate the collective wisdom of its practitioners. They help to ensure consistency across the wide spectrum of practitioners. That has to be true of something as important as information processing.

We have mentioned elsewhere the move towards empowerment and distributed systems. Empowerment means that the person responsible for an operating unit of an enterprise is free to obtain its services and resources anywhere. Where once information processing was done in-house, it is now just as likely to be out-sourced.

When information was once processed centrally the computer centre was well protected, both physically and logically. Indeed the protection of computer centres was the trigger for the development of corporate information security programmes. With information processing spread throughout the enterprise, the need for a central site vanishes. With it goes the ease of justifying the costs of high levels of security.

These two factors taken together mean that responsibility for information security is fragmented and put in the hands of people who have other responsibilities. Their mind set does not contain the same awareness of the need for security. Neither do they understand the interdependence of security and control measures.

The growth of legal, regulatory and contractual requirements for security create the need for a generally accepted set of controls and security measures. Words like due diligence and compliance with best practice can be satisfied by compliance with codes of practice. They provide the baseline needed for any comparison of actual with best practice.

Looking to the future we can see that information processing will become a basic skill for any skilled worker or manager. Where industries have their own codes of practice governing the way they operate, information security should become a sub-set.

Codes of practice must be formulated in such a way that audits can be performed to establish compliance.

Tasks

Development of:

- Review of current design practices and codes of conduct with the aim of generating a community wide standard for the safety of systems (4.5.)
- Codes of practice for the handling of non-classified information, as opposed to classified information. This should include rules for labelling of information. (4.7.)
- Guidelines to establish "cost of security" (4.9.)
- Assignment of responsibility and liability in global services (4.9.)
- Sector-specific codes of practice and base line controls, eg for:
  - finance
  - insurance

  - trade
  - medical
  - telecommunications
  - electronic service providers (including rules for inter-operation)
  - administrations (5.4.)

- Guidelines for the selection of security methodologies (5.5.)

- Code of Practice for data labelling (5.7.)

- Model contract clauses for contracts between service providers, TTPs and users, especially confidentiality service providers and services operating across national boundaries (5.9.1., 5.9.2., 5.9.3)

- Good practices for the operation of TTPs, specifically regarding availability, confidentiality, response times, rules of disclosure (6.1.2.)

- International guidelines for the accreditation and audit of TTPs (6.1.3.)

- International guidelines for

  - naming and certification
  - key management
  - directory services
  - legal services
  - time stamping
  - negotiable document transactions (6.1.4., to 6.1.9.)

- Rules for vendor declarations, as to the security of their products (6.2.3.)

- User and supplier obligations to report incidents (6.2.8.)

- Guidelines for the monitoring of compliance to codes of practice (7.4.)

- Rules for loss assessment (7.5.)

8.5 Specifications

Objectives

To develop specifications for the application of security, in order to ensure interworking, interoperation and mutual recognition.

Background

Functional specifications for products or services are documents that are to be used as parts of purchase specifications. They specify the functions of a solution and the required performance characteristics. Implementation aspects are only dealt with if they are particularly important for the fulfilment of a specific function. Specifications call up standards and profiles, as far as available. Options in the standards are resolved in specifications.

Common specifications for methodologies, eg evaluation, serve as a basis for mutual recognition.

Tasks

Development of:

- Specifications for solutions to confidentiality and integrity services (4.8.)
- Methodologies for the assessment of threats, vulnerabilities, and hazards for safety critical systems (4.11.)
- Development of methods of testing that enable standards of reliability to be ensured, including tests to destruction where appropriate (4.12.)
- Definition of requirements for fail-safe system architectures and implementations (4.12.)
- Specifications of security evaluations for safety critical environments
- Taxonomy of user requirements for enterprises, individuals and citizens (5.1., 5.2.)
- Identify and group access control scenarios, to determine levels of commonality (5.8.1.)
- Identify techniques, products, specifications and standards addressing access control, and associate them with the identified scenarios (5.8.1.)
- Identify parameters common to most or all of the above techniques, products, specifications and standards and investigate the feasibility of establishing common formats for them (5.8.1.)

- Identify the key features for coherence in the supporting infrastructure (5.8.1.)
- Define a limited number of basic access control mechanisms for pilot implementation (5.8.1.)
- Specification of a signature scheme (5.8.4.)
- Specification of application oriented integration of the signature scheme (5.8.4.)
- Specification of an Application Program Interface (API) for the signature scheme (5.8.4.)
- Specification of the use of multiple signatures (5.8.4.)
- Specification of key usage for integrity and confidentiality (5.8.5.)
- Specification for the practical use of digital signatures as a full equivalent to manual signatures (5.8.6.)
- Specification for the handling of electronically stored information (5.8.7.)
- Specification of an approach to confidentiality (5.9.1.)
- Assurance criteria for confidentiality service providers and operators (5.9.2.)
- Specification for the inter-operability of confidentiality services (5.9.3.)
- Specification for date and time stamping (6.1.8.)

8.6 Standards

Objective

Development of standards for IS.

Background

European security standards developed over the next decade will have a decisive influence on the technological structure of the entire European market and will change the conditions of trade in export markets and national markets.

The standards making infrastructure for the development of IT and telecommunication standards has become increasingly complex. The number of groups, the range of work items and the overall process at different levels of international, regional and national standardisation is a complex maze. Security standardisation is no exception to this situation. In general there is a reoccurring problem which is that of coordination between groups developing standards similar in nature and scope. Such coordination is necessary to avoid duplication of work and the unnecessary waste of resource, and to ensure that the standards that are developed are consistent and they form a coherent set.

At the European level the establishment of the Advisory Expert Group ITAEGV has provided an ideal mechanism for the coordination of security standards work within Europe. In addition, ITAEGV is in the process of developing a European Memorandum, M-IT-06, which is a Taxonomy and Directory of European Standardisation Requirements for Information Systems Security based on market driven requirements. This memorandum also contains a future work programme for security standardisation.

Hence Europe is now demonstrating through this action a clearly defined strategic stance on security standardisation. One that is demonstrating effective coordination, leadership and a market driven focused approach to standardisation.

Traditionally the principal contributors to standards making have been suppliers, designers and professionals. The end user of products and services has only been peripherally interested or involved. The end user has been concerned that standards have been used in relation to the products he buys but not greatly interested in what they are.

There is a need for a more effective mechanism and framework through which user interest is able to collectively express their requirements and priorities so that they can contribute to the standardisation process in a way which will balance the very strong interest of the supply industry.

This mechanism should be used to provide greater user input into the development of the European Memorandum, M-IT-06 (The Taxonomy and Directory of European Standardisation Requirements for Information Systems Security). This memorandum also contains a future work programme for security standardisation.

The long-term benefits of security standardisation requires investment by companies and users and as such they must be prepared to organise themselves more effectively to participate in the standards making process.

Tasks

- Define a solution to the specification, standardisation and licensing problem of cryptographic algorithms(5.8.4.).

Develop standards for:

- identify and group access control scenarios, to determine levels of commonality (5.8.1.)
- identify techniques, products, specifications and standards addressing access control, and associate them with the identified scenarios (5.8.1.)

- identify parameters common to most or all of the above techniques, products, specifications and standards and investigate the feasibility of establishing common formats for them (5.8.1.)
- identify the key features for coherence in the supporting infrastructure (5.8.1.)
- define a limited number of basic access control mechanisms for pilot implementation (5.8.1.)
- Digital signatures, including for application oriented integration and a general application programming interface (API) for integration of security services which could be easily integrated into any (almost) application (5.8.4.)
- Profile - or functional - standards to support CCITT X.509 (5.8.5.)
- Services and service provision. Ensure that the confidentiality services are compatible with existing communication standards and practices where possible (5.9.1.)
- Minimum requirements to ensure interoperability of procedure and operating practices for confidentiality services (5.9.3.)
- Evaluation criteria and methods (6.2.2.).

8.7 Products and Services

Objective

In order to facilitate a harmonious development of the provision of security of information systems in the Community for the protection of the public and of business interests, it will be necessary to develop a consistent approach as to its provision of security. Where independent organisations will have to be mandated, their functions and conditions will need to be defined and agreed and, where required, embedded into the regulatory framework. The objective would be to come to a clearly defined and agreed sharing of responsibilities between the different actors on a Community level as a prerequisite for mutual recognition.

Background

At present, the provision of security of information systems is well organised only for specific areas and limited to addressing their specific needs. The organisation on a European level is mostly informal, and mutual recognition of verification and certification is not yet established outside closed groups. With the growing importance of the security of information systems, the need for defining a consistent approach to the provision of security for information systems in Europe and internationally is becoming urgent. The most urgent needs identified relate to digital signatures and confidentiality services.

Tasks

- Verification of the existing provisions with respect to their conformance to the Internal Market Policy of the EC implying the removal of existing internal barriers and the avoidance of the formation of new technical barriers due to divergent application of IS rules, regulations and legislation (4.2.)

- Provision of IS to business and the public of solutions freely applicable throughout the Community and on a preferential basis at the international level (4.2.)

- An effective, internationally agreed, economic, ethical and usable solution to meet business, administration and personal needs including mechanisms for authorised interception and reporting of incidents and crimes adjusted to the conditions of the Internal Market, and to include the necessary equipment and software, but also an infrastructure of Trusted Third Parties. This will discourage "home-made" or other solutions (4.8.)

- Recommendation for the implementation for a public digital signature scheme for use by business, administrations and the general public (5.8.3.)

- Development of a general application programming interface (API) for integration of security services which could be easily integrated into most application (This could as well include codes which explain the intention of the applied signature.) (5.8.4.)

- Development of transaction-oriented multiple signature schemes (5.8.4.)

- Framework for the provision of trans-domain confidentiality services (Mechanisms are needed that provide for a defined way to pass from one domain to another. This will require collective or multilateral agreements for interoperation.) (5.9.2.)

- Demonstration of trans-European confidentiality services using a suitable application , eg the realisation of administrative telematics applications (5.9.3.)

- Trial service evaluations for existing telecommunication services (6.2.5.)

- Incident reporting system for Certification Bodies (6.2.8.)

8.8 Technology

Objective

Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future requirements for the security of information systems.

Background

Work on security of information systems would need to address development and implementation strategies, technologies, and integration and verification.

The strategic R&D work would have to cover conceptual models for secure systems (secure against compromise, unauthorised modifications and denial of service), functional requirements models, risk models and architectures for security.

Verification and validation of the security of the technical system and its applicability would be investigated through integration and verification projects.

In addition to the consolidation and development of security technology, a number of accompanying measures are required concerned with the creation, maintenance and consistent application of standards, and the validation and certification of IT and telecommunication products with respect to their security properties, including validation and certification of methods to design and implement systems.

The fourth RD&T Community Framework Programme might be one of the tools to foster co-operative projects at precompetitive and prenormative levels.

Tasks

- Demonstration, through pilot projects, that digital signatures can be used as equivalent to hand-written signatures (5.8.6.)
- Development of techniques for the establishment, handling and recording of Electronic Negotiable Documents (6.1.9.)
- Adapt to technological change:
  - Wide bandwidth telecommunications.

    Bandwidth will become a commodity on telecommunication systems. The added value in using it comes from the quality of service provided. One aspect of such quality is that of security. To provide security on wide band public switched networks, investment is needed that is focused on those aspects of security that are required by a) the telecoms service provider for his own purposes and b) the end user to support his application. Community wide and international specifications on security in ATM, SDH and associated signalling structures will be necessary.
  - Multi media applications and communications

    Multi media applications will integrate all known representations of information into files, documents, messages and displays. Representations such as voice, audio, still image, text, video and graphics will become interchangeably available from a range of equipments that users interact with, including mobile telephones, personal computers, television sets and personal communicators. All aspects of security must be incorporated for potential implementation an all of these systems in order that a user may implement a level of security service appropriate to the application and the environment.

A key issue is to maintain the "veracity" of the information transmitted. Veracity is the feature of a piece of information (eg a video sequence) to be true. Veracity is a wider concept than integrity which is only concerned with the protection of information during transmission and storage.

Another issue is concerned with the protection of information through copyright. Without suitable technical means to safeguard the interests of the information owner, the evolution towards the information society will be seriously hampered.

- Global teleconferencing

  Teleconferencing is becoming the substitute for travel. In order to make it really cost effective all the above applications, multimedia, mobility, access to mass data and if necessary access to one or more parties who are travelling in private vehicles need to be incorporated within the teleconferencing application. True geographic independence will come only if such an application works on a global scale and provides all the security services that are needed by the community of users. Such an application will demand the integration of the security services provided for each of the sub-applications alone. Specifications to allow such integration should be defined and the technology to provide the security functionality developed.

- Mobile services for applications.

  Mobility provides the end user with geographic independence. The price paid for this independence is infrastrucural information and process that allows his demands on the infrastrucural services to be met wherever he is. Such information and process has to, by design, have security features incorporated. At the community level extensions of the GSM concepts to allow all applications to function securely in the way telephony does on GSM will require significant technological investment.

- Mass data storage and communications in portable systems.

  Access to huge amounts of data from a mobile terminal will be essential. Such data needs to be communicated securely, whether it be held in volatile memory, in the form of mechanically read ROM or transmitted over a network. Specifications for securing such data need to be developed as do the necessary bulk encryption services for huge data volumes . The technology components of such services will be a major challenge and need to be defined now.

- Robotically controlled transportation mechanisms.

  Human involvement in controlling mass transportation mechanisms is already decreasing as technology becomes more reliable. If human involvement for individual transportation is to shrink in the same way then mass production of cost effective safety assured technologies will be essential. Collision avoidance

, guidance and navigation systems will be essential parts of every domestic vehicle and the requirements for the information safety and security critical elements of such systems need to be defined, standardised and developed.

8.9 Regulation and Legislation

Objective

Adjustment of national regulations and legislation to permit seamless interworking of trusted services.

Background

The provision of information security is seen to related in some areas closely to public order and defence issues. The related national regulations and legislations vary considerably. In order to avoid the creation of technical barriers to trade and communications outside the domains of internal order and national security, adjustments of legislation and regulations may be required in some countries.

Tasks

Development of a legal framework to address the following issues:

- Verification of the existing provisions with respect to their conformance to the Internal Market Policy of the EC implying the removal of existing internal barriers and the avoidance of the formation of new technical barriers due to divergent application of IS rules, regulations and legislation (4.2.)
- Clarification of the ownership and privacy issues surrounding biometric data (4.4.)
- Study the legal environment within which vendors and users of safety critical systems work, with the objective of harmonising that environment (4.5.)
- Need to provide business and the general public with an effective, economic and usable security solution to meet their needs including a mechanism for authorised interception (4.8.)
- Establishment of a network of Trusted Third Parties to provide user support and manage directories (4.8.)
- Clarification of responsibilities of the sector actors in general and in their relations within each other, with particular reference to open and distributed applications (4.10.)
- Agreement on management, TTPs, accreditation, auditing and relations with law enforcement agencies (5.6.)

- Clarification of the right to signature and the attached authority (5.8.3.)
- The legal functions of signatures need to be agreed EC-wide/internationally. Once this is achieved, it is possible to determine to what extent a code-of- practice will suffice. One issue to be addressed is the intended use of the digital signature, and the legal responsibility and liability of the signing entity with regard to the signed information (5.8.3.)
- Clarification of the conditions of acceptance of the authority of an electronic signature, eg for legally binding purposes, ie as substitute for hand-written original signatures (5.8.3.)
- Solution to the licensing problem of cryptographic algorithms (5.8.4.)
- Definition of minimum requirements to ensure interoperability, including standards, specifications, rules of procedure and operating practices for autonomous confidentiality services (5.9.3.)
- Alignment of national procurement policies concerning evaluated products (5.11.)
- Definition of the classes of information used and the types of damage that could be caused to the information owners (5.12.)
- Definition of the rights and duties of information ownership (5.12.)
- Development of guidance for owners of information as to the actions that they would have been expected to take to protect their assets and avoid negligence charges (5.12.)
- Development of the methods and procedures that should be used to establish information value (5.12.)
- Introduce or harmonise legislation to provide an appropriate framework for arbitration, supervision and litigation (6.1.2.)
- Adapt applicable legislation or regulations to provide an appropriate legal framework for use throughout the Community and in the relations with third countries (6.1.3.)
- Harmonisation of legislation on the legal status of evidence generated by any TTPs and especially on the intra- and extra- community recognition thereof. This probably implies the settlement of the accreditation question.
- Promotion of community-level information technology litigation services modelled after existing international bodies such as the International Chamber of Commerce (6.1.7.)
- Framework for international law relating to IS (7.1.)
- Development of international framework for private law, especially liability (7.2.)

8.10 Accreditation

8.10.1 Accreditation of Services

Objective

Evaluation of communication services.

Background

Common criteria for security evaluation are mainly focused on IT products and IT systems. However, there is a perceived need for criteria to support the evaluation of communication services. This later criteria may be considered as an extension to the current criteria or there may be a need to develop separate criteria.

The evaluation of a service and its subsequent accreditation will be a critical requirement in many user applications, in particular those that need to use trans-European communication services. The consistency, completeness and effectiveness of the security enhancements of communication services needs to be checked for an overall fitness for purpose. Hence there is a need for a framework for accreditation of communications services.

Tasks

- Establishment of a formal accreditation scheme for secure communication services (6.2.5.)
- Development of accreditation guidelines for the telecommunication sector (6.2.5.)
- Accreditation guidelines for the trusted network management (6.2.6.)

8.10.2 Accreditation of TTPs

Objective

Procedures for the accreditation and audit of TTPs.

Background

TTPs will need to interwork and communicate internationally to provide a service infrastructure to support a range of security services such as digital signature and confidentiality. TTPs will thus need to process, store and distribute a range of security-related information for the use and management of such services. This implies the need for a set of harmonised procedures for the accreditation and audit of TTPs in order to ensure mutual trust by the public in TTPs and the services they provide.

Tasks

- Development of international guidelines for the accreditation and audit of TTPs (6.1.3.)
- Adaptation of applicable legislation or regulations to provide an appropriate legal framework for use throughout the Community and in the relations with third countries (6.1.3.)

Annex: Recalling the Action Lines from the Council mandate

Action line I - Development of a strategic framework for the security of information systems

Issue

Security of information systems is recognized as a pervasive quality necessary in modern society. Electronic information services need a secure telecommunications infrastructure, secure hard- and software as well as secure usage and management. An overall strategy, considering all aspects of security of information systems, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world.

Objective

A strategically oriented framework has to be established to reconcile social, economic and political objectives with technical, operational and legislative options for the Community in an international context. The sensitive balance between different concerns, objectives and constraints are to be found by sector actors working together in the development of a common perception and agreed strategy framework. These are the are the prerequisites for reconciling interests and needs both in policy-making and in industrial developments.

Status and trends

The situation is characterized by growing awareness of the need to act. However, in the absence of an initiative to coordinate efforts, it seems very likely that dispersed efforts various sectors will create a situation which will de facto be contradictory, creating progressively more serious legal, social and economic problems.

Requirements, options and priorities

Such a shared framework would need to address and situate risk analysis and risk management concerning the vulnerability of information and related services, the alignment of laws and regulations associated with computer/telecommunications abuse and misuse, administrative infrastructures including security policies, and how these may be effectively implemented by various industries/disciplines, and social and privacy concerns (e.g. the application of identification, authentication, non-repudiation and possibly authorization schemes in a democratic environment).

Clear guidance is to be provided for the development of physical and logical architectures for secure distributed information services, standards, guidelines and definitions for assured security products and services, pilots and prototypes to establish the viability of various administrative structures, architectures and standards related to the needs of specific sectors.

Security awareness must be created in order to influence the attitude of the users towards an increased concern about security in information technology (IT).

Action line II - Identification of user and service provider requirements for the security of information systems

Issues

Security of information systems is the inherent prerequisite for the integrity and trustworthiness of business applications, intellectual property and confidentiality. This leads inevitably to a difficult balance and sometimes choices, between a commitment to free trade and a commitment to securing privacy and intellectual property. These choices and compromises need to be based on a full appreciation of requirements and the impact of possible options for the security of information systems to respond to them.

User requirements imply the security functionalities of information systems interdependent with technological, operational and regulatory aspects. Therefore, a systematic investigation of security requirements for information systems forms an essential part of the development of appropriate and effective measures.

Objective

Establishing the nature and characteristics of requirements of users and service providers and their relation to security measures of information systems.

Status and trends

Hitherto, no concerted effort has been undertaken to identify the rapidly evolving and changing requirements of the major actors for the security of information systems. Member States of the Community have identified the requirements for harmonization of national activities (especially of the "IT security evaluation criteria"). Uniform evaluation criteria and rules for mutual recognition of evaluation certification are of major importance.

Requirements, options and priorities

As a basis for a consistent and transparent treatment of the justified needs of the sector actors, it is considered necessary to develop an agreed classification of user requirements and its relation to the provision of security in information systems.

It is also considered important to identify requirements for legislation, regulations and codes of practice in the light of an assessment of trends in service characteristics and technology, to identify alternative strategies for meeting the objectives by administrative, service, operational and technical provisions, and to assess the effectiveness, user friendliness and costs of alternative security options and strategies for information systems for users, service providers and operators.

Action Line III - Solutions for immediate and interim needs of users, suppliers and service providers

Issues

At present it is possible to protect adequately computers from unauthorized access from the outside world by "isolation", i.e. by supplying conventional organizational and physical measures. This applies also to electronic communications within closed user group operating on a dedicated network. The situation is very different if the information is shared between user groups or exchanged via a public, or generally accessible, network. Neither the technology, terminals and services nor the related standards and procedures are generally available to provide comparable security for information systems in these cases.

Objectives

The objective has to be to provide, at short notice, solutions which can respond to the most urgent needs of users, service providers and manufacturers. This includes the use of common IT-security evaluation criteria. These should be conceived as open towards future requirements and solutions.

Status and trends

Some user groups have developed techniques and procedures for their specific use responding, in particular, to the need for authentication, integrity and non-repudiation. In general, magnetic cards or smart cards are being used. Some are using more or less sophisticated cryptographic techniques. Often this implied the definition of user-group specific "authorities". However, it is difficult to generalise these techniques and methods to meet the needs of an open environment.

ISO is working on OSI Information System Security (ISO DIS 7498-2) and CCITT in the context of X400. It is also possible to insert security segments into the messages.

Authentication, integrity and non-repudiation are being addressed as part of the messages (EDIFACT) as well as part of the X400 MHS.

At present, the Electronic Data Interchange (EDI) legal framework is still at the stage of conception. The International Chamber of Commerce has published uniform rules of conduct for the exchange of commercial data via telecommunications networks.

Several countries (e.g. Germany, France, the United Kingdom and the United States) have developed, or are developing, criteria to evaluate the trustworthiness of IT and telecommunication products and systems and the corresponding procedures for conducting evaluations. These criteria have been coordinated with the national manufacturers and will lead to an increasing number of reliable products and systems starting with simple products. The establishment of national organizations which will conduct evaluations and offer certificates will support this trend.

Confidentiality provision is considered by most users as less immediately important. In the future, however, this situation is likely to change as advanced communication services and, in particular, mobile services will have become all-pervasive.

Requirements, options and priorities

It is essential to develop as soon as possible the procedures, standards, products and tools suited to assure security both in information systems as such (computers, peripherals) and in public communications networks. A high priority should be given to authentication, integrity and non-repudiation. Pilot projects should be carried out to establish the validity of the proposed solutions. Solutions to priority needs on EDI are looked at in the TEDIS programme within the more general content of this action plan.

Action line IV - Development of specifications, standardization, evaluation and certification in respect of the security of information systems

Issues

Requirements for the security of information systems are pervasive and as such common specifications and standards are crucial. The absence of agreed standards and specifications for IT security may present a major barrier to the advance of information-based processes and services throughout the economy and society. Actions are also required to accelerate the development and use of technology and standards in several related communication and computer network areas that are of critical importance to users, industry and administrations.

Objective

Efforts are required to provide a means of supporting and performing specific security functions in the general areas of OSI, ONP, ISDN/IBC and network management. Inherently related to standardization and specification are the techniques and approaches required for verification, including certification leading to mutual recognition. Where possible, internationally agreed solutions are to be supported. The development and use of computer systems with security functions should also be encouraged.

Status and trends

The United States, in particular, has taken major initiatives to address the security of information systems. In Europe the subject is treated in the context of IT and telecommunications standardization in the context of ETSI and CEN/CENELEC in preparation of CCITT and ISO work in the field.

In view of growing concern, the work in the United States is rapidly intensifying and both vendors and service providers are increasing their efforts in this area In Europe, France, Germany and the United Kingdom have independently started similar activities, but a common effort corresponding to the United States is evolving only slowly.

Requirements, options and priorities

In the security of information systems there is inherently a very close relationship between regulatory, operational, administrative and technical aspects. Regulations need to be reflected in standards, and provisions for the security of information systems need to comply in a verifiable manner to the standards and regulations. In several aspects, regulations require specifications which go beyond the conventional scope of standardization, i.e. include codes of practice. Requirements for standards and codes of practice are present in all areas of security of information systems, and a distinction has to be made between the protection requirements which correspond to the security objectives and some of the technical requirements which can be entrusted to the competent European standards bodies (CEN/CENELEC/ ETSI).

Specifications and standards must cover the subjects of security services of information systems (personal and enterprise authentication, non-repudiation protocols, legally acceptable electronic proof, authorisation control), their communication services (image communication privacy, mobile communications voice and data privacy, data and image data-base protection, integrated services security), their communication and security management (public/private key system for open network operation, network management protection, service provider protection) and their certification (assurance criteria and levels, security assurance procedures for secure information systems).

Action line V - Technological and operational developments in the security of information systems

Issues

Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future requirements for the security of information systems is a prerequisite for the development of the services market and the competitiveness of the European economy as a whole.

Any technological developments in the security of information systems will have to include both the aspects of computer security and security of communications as most present-day systems are distributed systems, and access to such systems is through communications services.

Objective

Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future requirements for the security of information systems.

Requirements, options and priorities

Work on security of information systems would need to address development and implementation strategies, technologies, and integration and verification.

The strategic R&D work would have to cover conceptual models for secure systems (secure against compromise, unauthorized modifications and denial of service), functional requirements models, risk models and architectures for security.

The technology-oriented R&D work would have to include user and message authentication (e.g. through voice-analysis and electronic signatures), technical interfaces and protocols for encryption, access control mechanisms and implementation methods for provable secure systems.

Verification and validation of the security of the technical system and its applicability would be investigated through integration and verification projects.

In addition to the consolidation and development of security technology, a number of accompanying measures are required concerned with the creation, maintenance and consistent application of standards, and the validation and certification of IT and telecommunication products with respect to their security properties, including validation and certification of methods to design and implement systems.

The third RD&T Community Framework Programme might be used to foster cooperative projects at precompetitive and prenormative levels.

Action line VI - Provision of security of information systems

Issues

Depending on the exact nature of the security features of information systems, the required functions will need to be incorporated at different parts of the information system including terminals/computers, services, network management to cryptographic devices, smart cards, public and private keys, etc. Some of these can be expected to be embedded in the hardware or software provided by vendors, while others may be part of distributed systems (e.g. network management), in the possession of the individual user (e.g. smart cards) or provided from a specialised organization (e. g. public/private keys).

Most of the security products and services can be expected to be provided by vendors, service providers or operators. For specific functions, e.g. the provision of public/private keys, auditing authorization, there may be the need to identify and mandate appropriate organizations.

The same applies for certification, evaluation and verification of quality of service which are functions which need to be addressed by organizations independent of the interests of vendors, service providers or operators. These organizations could be private, governmental or licensed by government to perform delegated functions.

Objective

In order to facilitate a harmonious development of the provision of security of information systems in the Community for the protection of the public and of business interests, it will be necessary to develop a consistent approach as to its provision of security. Where independent organizations will have to be mandated, their functions and conditions will need to be defined and agreed and, where required, embedded into the regulatory framework. The objective would be to come to a clearly defined and agreed sharing of responsibilities between the different actors on a Community level as a prerequisite for mutual recognition.

Status and trends

At present, the provision of security of information systems is well organized only for specific areas and limited to addressing their specific needs. The organization on a European level is mostly informal, and mutual recognition of verification and certification is not yet established outside closed groups. With the growing importance of the security of information systems, the need for defining a consistent approach to the provision of security for information systems in Europe and internationally is becoming urgent.

Requirements, options and priorities

Because of the number of different actors concerned and the close relations to regulatory and legislative questions, it is particularly important to pre-agree on the principles which should govern the provision of the security of information systems.

In developing a consistent approach to this question, one will need to address the aspects of identification and specification of functions requiring, by their very nature, the availability of some independent organizations (or interworking organizations). This could include functions such as the administration of a public/private key system.

In addition, it is required to identify and specify, at an early stage, the functions which in the public interest need to be entrusted to independent organizations (or interworking organizations). This could, for example, include auditing, quality assurance, verification, certification and similar functions.

OJ No L 123, 8.5.1992, p.19

SOG-IS Opinion of 17.11.92 on objectives, scope and approach

Information Security is concerned with the protection of information stored, processed or transmitted in electronic form, against deliberate or accidental threats.

Information is acquired, communicated, processed and stored by Information Services. Electronic Information services need a secure telecommunication infrastructure, secure terminals (including processors and data bases) as well as secure usage. The management of the service provision itself must also and foremost be secure. Therefore the approach to information security starts form an analysis of the needs of an individual or organisation for Information Services.

92/242/EEC

This danger has already been identified and OECD Member Countries have, in the context of Protection of Privacy and Transborder Data Flow of Personal Data, recognised the risk of new technical barriers forming. They have therefore agreed to endeavour to remove and to avoid to create in the name of privacy protection, unjustified obstacles to transborder flows of personal data, co-operate in the implementation of the Guidelines and agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.