September/2001

57

ISSN: 1025-9384

5 EURO ΕΥΡΩ

The IPTS REPORT

EDITED BY THE INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS)
AND ISSUED IN COOPERATION WITH THE EUROPEAN S&T OBSERVATORY NETWORK

SPECIAL ISSUE: ASPECTS OF CYBER-SECURITY

EUROPEAN COMMISSION
Joint Research Centre

ENGLISH VERSION

ABOUT THE IPTS REPORT

The IPTS Report is produced on a monthly basis - ten issues a year to be precise, since there are no issues in January and August - by the Institute for Prospective Technological Studies (IPTS) of the Joint Research Centre (JRC) of the European Commission. The IPTS formally collaborates in the production of the IPTS Report with a group of prestigious European institutions, forming with IPTS the European Science and Technology Observatory (ESTO). It also benefits from contributions from other colleagues in the JRC.

The Report is produced simultaneously in four languages (English, French, German and Spanish) by the IPTS. The fact that it is not only available in several languages, but also largely prepared and produced on the Internet's World Wide Web, makes it quite an uncommon undertaking.

The Report publishes articles in numerous areas, maintaining a rough balance between them, and exploiting interdisciplinarity as far as possible. Articles are deemed prospectively relevant if they attempt to explore issues not yet on the policymaker's agenda (but projected to be there sooner or later), or underappreciated aspects of issues already on the policymaker's agenda. The multi-stage drafting and redrafting process, based on a series of interactive consultations with outside experts guarantees quality control.

The first, and possibly most significant indicator, of success is that the Report is being read. The issue 00 (December 1995) had a print run of 2000 copies, in what seemed an optimistic projection at the time. Since then, readership of the paper and electronic versions has exceeded the 50,000 mark. Feedback, requests for subscriptions, as well as contributions, have come from policymaking (but also academic and private sector) circles not only from various parts of Europe but also from the US, Japan, Australia, Latin America, N. Africa, etc.

We shall continue to endeavour to find the best way of fulfilling the expectations of our quite diverse readership, avoiding oversimplification, as well as encyclopaedic reviews and the inaccessibility of academic journals. The key is to remind ourselves, as well as the readers, that we cannot be all things to all people, that it is important to carve our niche and continue optimally exploring and exploiting it, hoping to illuminate topics under a new, revealing light for the benefit of the readers, in order to prepare them for managing the challenges ahead.

THE IPTS REPORT

57

SEPTEMBER 2001

EDITED BY THE INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS)
And issued in Cooperation with
the European S&T Observatory Network

PUBLISHED BY THE EUROPEAN COMMISSION
Joint Research Centre
ISSN: 1025-9384
Catalogue Number LF-AA-01-057-EN-C
DEPOT LEGAL: SE-1937-95

DIRECTOR
Jean-Marie Cadiou

EXECUTIVE EDITOR
Dimitris Kyriakou

EDITORIAL BOARD
B. Clements, G. Fahrenkrog, J. Gavigan, M. González, H. Hernández, D. Kyriakou, I. Maghiros (Production Manager), P. Sørup, A. Soria, C. Tahir.

PRODUCTION
CINDOC-CSIC/L&H Spain

PRINT
Graesal

TRANSLATION
CINDOC-CSIC/L&H Spain

THE IPTS REPORT
is published in the first week of every month, except for the months of January and August. It is edited in English and is currently available at a price of 50 EURO per year, in four languages: English, French, German and Spanish.

SUBSCRIPTIONS
For a subscription to The IPTS Report, or to amend an existing subscription, please write with full details to:
The IPTS Report Secretariat
IPTS, JRC Sevilla
World Trade Center
Isla de la Cartuja
E-41092 Sevilla, Spain
Tel: +34-95-448 82 97
Fax: +34-95-448 82 93
E-mail: ipts_secr@jrc.es
Web address: www.jrc.es/iptsreport/subscribe.html

CONTENTS

Special Issue: Aspects of Cyber-Security

EDITORIAL

Cyber-Security Issues

Bernard Clement, Laurent Beslay and Duncan Gilson, *IPTS*

Cyber-security is a broad issue which is becoming increasingly important as computer networks become more widespread. It encompasses computer- and network-related crime, privacy issues, trust and confidence, and dependability of critical infrastructures. At the level of individual Member States, European objectives for harmonization and integration, in conjunction with the eEurope project, have created the obligation to ensure access to pan-European infrastructure such as telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, and emergency services. These critical infrastructures are increasingly dependent on ICT infrastructures. In their drive for greater efficiency companies and organizations are computerizing and networking their systems, thus making these systems increasingly vulnerable to attack. Moreover, the inexorable drive towards standardization and open platforms that characterizes systems in the civilian field increases their vulnerability in that a standardized system is an easier target to hit. One of the lines of research that has been identified is the need to take greater account of a range of infrastructure issues, and in particular critical infrastructures issues, in order to build a stronger partnership between the public and private sector. Unlike the surveillance vs. privacy debate, this is an area where the interests of the public and private spheres coincide.

Cyber-security is also an important issue for electronic commerce. The three main security-related barriers to the uptake of e-commerce by users have been identified as being: 1) the technological inadequacies in the hardware and software providing security; 2) the limited diffusion of secure processes; and, 3) the perception of insecurity (i.e. user trust and confidence). The main security threats to computer networks can be subdivided into those traditional criminal activities that have simply shifted to the Internet as an alternative channel, and those activities that specifically target the network. Clearly, overcoming these problems will be a necessary part of the development of e-commerce and the information society in general. For business, a major issue today is to create a model for identification (saying who you are) and authentication (proving you are who you say you are) that not only works reliably, but inspires sufficient trust in users and merchants alike to encourage their use of e-commerce. On the users' side, the information that businesses collect about their customers or visitors to their web sites is an area in which conflicts may arise between the interests of businesses wishing to target their products and services, and the desire of individuals to ensure their privacy and/or anonymity.

Estimating the incidence, scale and cost of cybercrime represents one of the most important challenges lawmakers face when dealing with computer- and network-related crime. It is clearly essential to evaluate the scale and impact of

cybercrime activity in order to define the types of measures to be taken and ensure their proportionality. Measurement is subsequently necessary to assess the effectiveness of the measures taken. However, for a mixture of economic and psychological reasons cybercrime is probably greatly under-reported. Since it strikes at the heart of the notion of technological security, firms may well be reluctant to admit that apparently sophisticated measures designed to protect the interests of their customers have been unravelled with apparent ease by an errant teenager. Cyber attacks on bank accounts are likely to have a much greater direct impact on the customer than traditional bank robberies and so be liable to undermine user confidence. This sort of consideration is likely to influence banks' policy on security and on handling complaints of irregularities. Although difficult, obtaining reliable statistics is essential if realistic cost-benefit assessment of the risks is to be made.

Cybercrime: motive, opportunity and vulnerability

Cybercrime, as in all crime, is made possible by the confluence of three factors: motive, opportunity and vulnerability. When the value is sufficient to incite motive, the influence of the two other factors depends specifically on the available technologies - in the case of cybercrime, on the availability of new information and communications technologies (ICTs).

As has been predicted,[1] an increasing proportion of the activities of media, banking, and government services have been digitized. This means that these activities are not only evolving into fully computerized processes but are becoming part of a fully interconnected network environment. Paradoxically, it is this powerful technological combination which represents a key point of weakness, as it has enabled the creation of a virtual world which provides both the opportunity and vulnerability necessary for cybercrime to prosper. The criminal fraternity will tend to shift its attention to the point where maximum value meets maximum vulnerability, thus as value increasingly moves onto digital networks, greater efforts will be needed to protect that value, one way or another, against the attentions of criminal elements.

To some extent, the information revolution can be regarded as an outcome and logical continuation of the process of the digitization[2] of economic activity. Thus, some aspects of electronic commerce will in part simply substitute for traditional commerce, and insofar as this is the case, cybercrime and cyber-criminals will partially replace traditional crime and traditional criminals, although perhaps with differing degrees of sophistication. In this sense, some aspects of cyber-criminality will be new, but others have a familiar ring to those involved in fighting crime.

Another facet of the problem, however, adds to the emerging complexity. E-commerce may be attractive to businesses initially because it enables them to cut costs, increase efficiency and gain a temporary competitive advantage. But its real attractiveness lies in the long-term potential it has for transforming ways of doing business to an extent that adds new value to the economy. As the transformation potential of e-commerce materializes, its substitutional effects diminish, and a new economy replaces the old. Since crime naturally targets sources of value, it is only to be expected that with the digitization of value comes the digitization of crime. New value creation, and the value itself (electronic cash is a simple example) thus constitute the new target for criminal activity.

Ironically, the emergence of "net crime" today may be seen a positive sign for E-Commerce as it demonstrates perhaps more effectively than any media hype that electronic business is generating economic value.

The Internet as vehicle or target

The references made earlier to the substitutional and new effects of e-commerce are reflected in what we perceive as two fundamental categories of cybercrime:

- traditional types of crime in which the Internet is merely a vehicle for criminal activity;
- attacks against the network in which Internet itself becomes the target.

Examples of the vehicle category include the unauthorized transfer of a bank balance, or the sale and distribution of child pornography. While these are crimes which have a bricks-and-mortar equivalent, there is no doubt that use of the Internet gives them a new scale and dimension. Examples of Internet as a target include the many instances where websites have been temporarily shut down as a result of cyber attacks (February 2000, Yahoo, Ebay, etc.) using various means, including viruses. However, this is more cyber-vandalism than cyber-robbery, and it will be necessary to identify profitable cybercrime scenarios in areas where the Internet is the source and sink of value in e-commerce transactions. Clearly intellectual property, industrial espionage, misuse of personal information, etc. are all areas in which there are potential impacts.

Law Enforcement in Cyberspace

The global and trans-national character of the Internet, and the difficulties in providing effective protection, give some idea of cyber-criminals' theatre of operations. The absence of frontiers, and the virtual guarantee of anonymity combine to provide new opportunities for disguise and new places of refuge for the wrongdoer. Among the complicating factors, that of national sovereignty is perhaps the most thorny. Cybercrime can easily be committed remotely from another part of the world where different jurisdictions and legal standards apply. Legal wrangles may arise as to the actual location of the crime if perpetrator and victim fall under two different jurisdictions. Moreover, the investigative powers or capabilities of each of the countries may differ, making cases difficult to prosecute even with the full cooperation of the authorities in all the countries concerned. In many cases, the normal instruments of policing and enforcement may no longer be adequate to uphold the law when faced with these challenges. The forces of law and order can no longer count on their traditional investigative capabilities, which are increasingly being rendered obsolete by the new technology. Such an absence of effective legal protection contributes to creating a favourable climate for cybercrime. As the recent Commission Communication on cybercrime states, "the speed, mobility and flexibility of computer crime challenge the existing rules of criminal procedural law"[3] (for some recent directives and communications see Box 1).

Box 1. Computer and network security related directives and communications from the European Commission

- Communication to the Council and the European Parliament entitled Creating a *Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, (COM(2000)890) 26/1/2001.
- Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: *Network and Information Security: Proposal for a European Policy Approach* (COM(2001) 298) 06/06/2001.
- Commission report entitled: *e-EUROPE- an Information Society for All'* progress report for the Special European Council on Employment, Economic reforms and Social Cohesion: Lisbon 23rd and 24th March 2000 (COM (2000) 130).
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 *on certain legal aspects of information society services, in particular electronic*

commerce, in the Internal Market ("Directive on electronic commerce")
- Directive 1999/93/EC of 13 December 1999 *Establishing a common framework for electronic signatures*
- Commission Communication on *Ensuring security and trust in electronic communication,* 8 October 1997, COM (1997) 503 final.
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 *concerning the processing of personal data and the protection of privacy in the telecommunications sector*
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
- Council Directive 91/308/EEC *on prevention of the use of the financial system for the purpose of money laundering*
- *Proposal for a directive on Distance selling of financial services* COM (1999) 385, July 1999.

In addition to the above, the European Commission's JRC is engaged in raising awareness and promoting consensus on issues of mutual concern among a broad spectrum of interested parties across European and international borders. The discussions at the recent workshop on cybercrime focused on the technical and jurisdictional issues, as well as the broader political implications.

The erosion of the constraints of time and distance caused by these new technologies therefore gives renewed emphasis to the problem of non-harmonized legal environments. One clear example is the problem of lawful interception of communications, both in terms of the capability and grounds for such interception. As the same Commission Communication states, "New technologies make it essential that Member States work together if they are to maintain their capabilities for lawful interception of communications."[4]

Skills shortages

The need to protect networks and data from attack or misuse is leading to increased demand for people with the right skills and training. Today, a network administrator not only has to have operating system management skills, but also needs to know about viruses, cryptography, authentication processes, etc. At the same time, law enforcers not only need traditional crime investigation skills but they also need to know how to collect and preserve digital evidence relating to either cyber-crime or traditional offences. Clearly, the highly technical nature of cyber crime and fraud also underscores the need for a close partnership between public and private sectors in defining and implementing training policies and programmes.

These problems underline the importance of taking measures to ensure the proper education and training of law enforcement personnel in the use of advanced technologies. New "Cyber Police" will in future be skilled in the application and use of information and communication technologies, operating systems, electronic surveillance methods and cryptography. The new skills will sit side-by-side with the more traditional policing capabilities of analysis, investigative methods and familiarity with the practices and motives of cyber-criminals, all of which will continue to be required.

However, the forensic processes involved in identifying and collecting evidence will be completely new, and so new training needs will be created. The scene of a cybercrime case may well be virtual, but its proof still constitutes a critical parameter for the success of an investigation. Thus issues such as data recovery, data source identification, Internet traces, computer evidence, and the question of harmonization of forensic methods for consistency of approach will also arise.

Law Enforcement and Privacy - Striking the Right Balance

The dilemma described above needs to be resolved in a way which broadly meets the interests of both public and private sectors. Using information and communication technologies to fight cybercrime can have some unfortunate side effects. While a climate of confidence in their use is essential for the development and growth of electronic commerce, technologies used for investigation and surveillance in order to protect citizens from crime may in fact threaten their privacy and human rights. The challenge for policymakers therefore is to effectively reduce cybercrime while preserving the rights of individuals to privacy in an increasingly interconnected network environment. Perhaps a form of the precautionary principle can be applied here. The construction of scenarios on the impact of cybercrime around such themes as electronic payment systems, ambient intelligence and ubiquitous computing could contribute to making the right technology and policy choices for the future.

The expansion of the Internet in domestic and mobile networks, and the multiplication of the number of types and modes of connection, will make the individual the point of convergence of a whole gamut of networked services. Identification will become an essential and critical function for users as they move around within an intelligent networked environment. However, excessively "strong" identification raises privacy concerns. Thus policymakers will need to be alert to threats to individual privacy and balance the needs of law enforcers wishing to monitor and detect potentially criminal activity with the legitimate right of privacy citizens should be able to enjoy in a democratic society.

Public and Private Sectors – A New Relationship?

The emergence of cybercrime also calls for a new look at the relationship between public authorities and the private sector. Perhaps the clearest illustration of this is to be found in the area of cryptography. As the single most important privacy-enhancing technology, cryptography imparts confidentiality, integrity and authentication to all forms of electronic communication. In contrast to past practice, most of the R&D effort in this area now comes from the private sector. Nevertheless, since such systems can be used for illegal activities, public authorities maintain an element of control over their use and distribution. This creates something of a dilemma, in that on the one hand, those promoting the growth of e-commerce are calling for the widest possible application of cryptography to protect the integrity of electronic transactions, in pursuit of creating a climate of confidence in their use. On the other, law enforcement agencies must be in a position to gain access to communications when necessary in order to combat cybercrime. Moreover, the public sector is equally dependent on a climate of confidence to enable development of the electronic services it provides citizens, and which are equally vulnerable to cybercrime. A further illustration of the difficulty created by cryptography is the blurring of distinctions between protecting national security and protecting national economic interests. Rather than being considered strategic weapons of defence, as was the case in cold-war days, these brands of technology are now regarded as essential instruments for protecting commercial confidentiality in an increasing global competitive marketplace.

Global Initiatives on Cybercrime

Many international initiatives on cybercrime are already underway. From 22 to 24 May 2001 the G8 held a meeting in Tokyo (followed by several working group meetings) and reconfirmed the importance of the relationship between governments and the private sector for a coordinated response to cybercrime. The OECD has opted for a more technology-based approach, with its May

1997 guidelines on cryptography policy.[5] In April 2000, the 41-member Council of Europe issued a draft International Convention on the fight against cybercrime, consisting of both technical and legal provisions. In the EU, the Council adopted a resolution in 1995[6] (revised in 1998-99) aimed at harmonizing the rules on the legal interception of telecommunications.

The Workshop (see Box 2) was particularly timely because it came in the wake of the adoption by the European Commission of its Communication on *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*. Later in June, with a communication from the Council, the European Commission sought to give further impetus to security initiatives for networks and information. It is worth noting that these initiatives generally address the current perception of the kinds of protective measures needed, based on the way new technologies are being applied today. It could be claimed that such a perspective is not sufficiently forward-looking, and that as technology evolves to hitherto unknown levels of sophistication, there is a risk of today's approaches becoming rapidly obsolescent, and thus ineffective.

Box 2. Potential lines of research

- **The lack of accurate statistics.** Detailed information on the extent of the phenomenon is needed. Statistics are essential both for the public sector, which has to define security policy and determine the extent to which the law is observed, and for the private sector, so it can include this risk when defining economic models. Research is needed in order to identify current obstacles to data gathering, to work out an operational system of anonymous collection of cybercrime statistics and to define their requirements.
- **Best practice in forensic methods and quality control of digital evidence**. Work is needed to define intangible evidence and set procedures for its collection.
- **Standardization procedures**, including methods for the anonymous reporting of crime statistics to compensate for the lack of statistics.
- **Cybercrime prevention methods**, including information, education and awareness campaigns at all educational levels, for a detailed study of prevention measures.
- **Risk assessment methodologies**, essential for gaining greater understanding of how cybercrime operates.
- **Universal definitions of cybercrime**, to enable co-ordination and harmonization initiatives.
- **Cybercrime impact assessments** in national security, the digital economy and the safeguarding of essential civil infrastructure.
- The need to find a way of **exchanging information** among law enforcement authorities, industry and users.
- Understanding the **impact of regulatory measures** in this area (liability versus criminal law) The relationship between intention in legislation, treaty negotiation and the effect that it will have once finished, enacted, adopted, applied, and enforced.
- The **security of end-user systems**
- **Legal liability** of software manufacturers in the event of negligent supply of security services or products

Notes

1. Being digital, Nicholas Negroponte, published by Alfred A. Knopf, Inc., New York, 1995.
2. Digitisation in this sense means a combination of computerisation (already well-established, though now more cost-effective and powerful) and communications (now cheaper, faster, easier, popular).
3. Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, European Commission, Brussels, to be adopted.
4. Ibid.
5. Guidelines for cryptography policy, OECD, 1997.
6. Council Resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 4.11. 1996, pp. 1– 6).

Contact

Laurent Beslay, IPTS
Tel.: +34 954 488 206, fax: +34 954 488 208, e-mail: **laurent.beslay@jrc.es**

Striking a Balance between Cyber-Crime Prevention and Privacy

Andreas Pfitzmann, *Dresden University of Technology* and
Marit Köhntopp, *Independent Centre for Privacy Protection*

Issue: A balance between cyber-crime prevention and the desire to ensure privacy is urgently needs to be struck. However, it is unclear to what extent this is possible using either the ICTs (Information and Communications Technology) available today or likely to become available in the near future.

Relevance: Privacy is a concern both for individuals and for democratic society as a whole. If people feel they are being spied upon, they will tend not to express themselves freely or act according to their own interests. As well as privacy, security is also a basic need for human beings. In a world where cyber-crime is becoming more prominent and its effects are increasingly serious, it is important to look for ways that prevent cyber-crime as far as possible without undermining the concept of privacy and security.

Introduction

The volume of digital communication has increased in line with the spread of the Internet as a global network. Nearly all this communication is lawful, but computer networks and electronic information may also be used to commit criminal offences. The concept of **cyber-crime** can be subdivided into two distinct areas:

- ordinary crime which makes use of the communications networks, and
- new forms of crime specific to computer networks.

In this article we will focus on cyber-crime prevention rather than limiting our view to cyber-crime prosecution. However, the methods used to enable prosecution may have a crime preventing effect. After stating some of the basic facts of ICT security, we discuss whether a balance can be struck between cyber-crime prevention and prosecution on the one hand and privacy on the other.

To begin our discussion of whether this balance can be struck, it is necessary to first define the underlying assumptions of our argument. Realistically, we have to assume that only partial cooperation between states and only the partial cooperation of industry will be possible. However, at the same time we have to accept that national borders will effectively be open to ICT, know how, and information (assuming world-wide trade and communication).

Against this backdrop, we have to consider the (net) effects on individuals, the economy, and so-

The concept of cyber-crime can be subdivided into criminal activities which use information and communications technologies as a tool or vehicle for traditional crimes, and those criminal activities which target networks or are specific to them

Security measures to protect computers and networks may be implemented multilaterally, to cover all the parties concerned, unilaterally by individual parties, bilaterally between parties wishing to interoperate, and trilaterally, when third party certification agencies, for instance, are involved

ciety that may be anticipated from each proposed ensemble of legal regulations and their prospective influence on ICT development, deployment, operation, and use.

In our search for a balance between the two conflicting aspects of this problem, we first have to look at today's ICT security technologies and at proposed cyber-crime prevention and prosecution methods.

Currently available security technologies

In order to help prevent cyber-crime, users should protect their computer systems and their data (including their transaction data and communication trails) against attacks. When discussing security technologies there are a number of configurations of the parties involved that can be considered.

The broadest arrangement is *Multilateral Security*, which means providing security for all parties concerned, requiring from each party only minimal trust in the honesty of the other parties:

- Each party has its particular *protection goals*.
- Each party can *formulate* its protection goals.
- Security conflicts are recognized and compromises *negotiated*.
- Each party can *enforce* its protection goals within the agreed compromise.

In the same way as the enlightenment paved the way for alternatives to superstitious world views and authoritarian political systems, technology for multilateral security has the potential to free users of ICT systems from the lack of self-determination that results from their lack of security.

Some of these technologies can unilaterally be employed by various parties. To use others, bilateral cooperation is needed, e.g. the cooperation of both communication partners. For some, trilateral cooperation is required. One example is that of legally binding digital signatures, which not only require the cooperation of the (at least two) communicating parties, but additionally at least one trusted third party for the certification of public keys. For other technologies, multilateral cooperation between a large number of independent parties may even be necessary. We will use this distinction to structure a short overview of what is known about technology for (multilateral) security, providing pointers to the relevant literature (Pfitzmann, 2000).

Unilateral Technologies

Unilateral technologies are technologies that each party can decide upon for itself. Therefore, neither coordination nor negotiation is needed concerning their use. Important unilateral technologies for multilateral security are:

- *Tools to help even inexperienced users* to formulate all their protection goals, if necessary for each and every application or even each and every action (Pfitzmann, 98, and Wolf, 2000).
- *(Portable) devices which are secure for their users* in order to bootstrap security. The devices need at least minimal *physical protection* comprising direct input/output with their users (Pfitzmann, 1999) and, if they are multipurpose, an *operating system* providing fine-grained access control and administration of rights for applications, adhering to the principle of least privilege. This is essential to limit the spread of Trojan horses, and can prevent computer viruses completely.
- *Encryption* of local storage media to conceal and/or authenticate its contents.
- *Hiding* of secret data in local multimedia contents or in the local file system (Anderson, 1998) using steganographic techniques, not only to conceal the contents of the secret data, but also its very existence.

- *Watermarking* or *fingerprinting* digital data using steganographic techniques to help prove authorship or copyright infringements.
- Using only *software* whose *source code is published and well checked* or the *security of which is certified* by a trustworthy third party having access to the complete source code and all tools used for code generation. The best technique is to combine both approaches with regard to as much of the software as possible. It is only by using at least one of these two approaches that you can be reasonably certain that the software you use does not contain Trojan horses. More or less the same applies to *hardware* where all sources and tools used for design and production are needed as well to check for the absence of Trojan horses.

Unilateral security options include secure portable devices, encryption of locally stored data, data concealment, watermarking and use of open source or certified software

Bilateral Technologies

Bilateral technologies can only be used if the communication partners cooperate. This means that some coordination and negotiation is needed concerning their use.

Important bilateral technologies for multilateral security are:

- *Tools to negotiate* bilateral protection goals and security mechanisms, (Pfitzmann, 1998).
- *Cryptographic mechanisms* and *steganographic mechanisms* to secure the communication content (see Figs. 1 and 2).

Bilateral technologies include tools for negotiating security mechanisms and cryptographic and steganographic mechanisms for securing content

Trilateral Technologies

Trilateral technologies can only be used if a third party is involved to fulfil a specific task for the other participating parties. This means that more coordination and negotiation is needed concerning their use compared with unilateral – and in most cases as well, bilateral – technologies. Important trilateral technologies for multilateral security are:

- *Tools to negotiate* trilateral security mechanisms, e.g. for accountability.
- A *public-key infrastructure* (PKI) to provide users with certified public keys of other users to test their digital signatures and to give users the ability to revoke their own public key if the corresponding private key has been compromised.
- *Security gateways* to bridge incompatibilities between security mechanisms or details. Security gateways work well for integrity and accountability mechanisms, but are of questionable value for confidentiality and anonymity mechanisms. Of course, security gateways cannot bridge incompatibilities between protection goals.

Figure 1. Cryptography to achieve confidentiality and integrity of communication contents

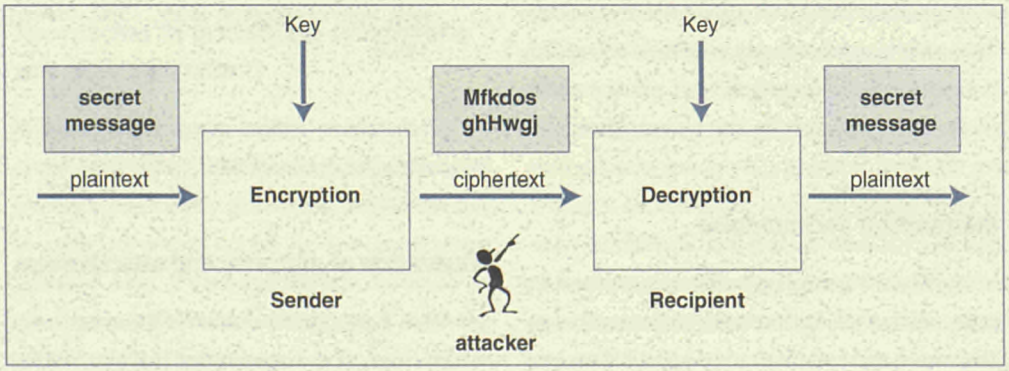
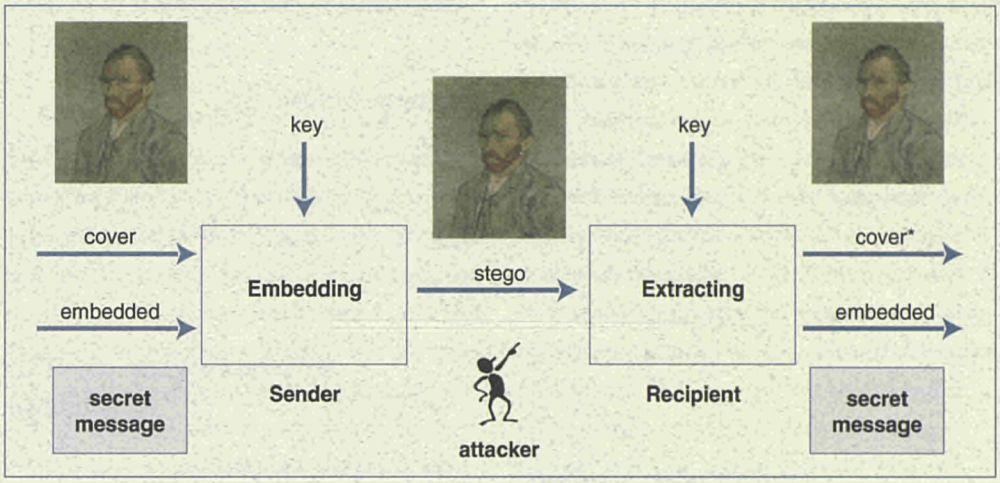


Figure 2. Steganography to achieve hiding, i.e. secrecy of confidential communication contents



Trilateral security technologies include public key infrastructure techniques which can use certified public keys, security gateways, and digital pseudonyms

- Mechanisms to provide for *digital pseudonyms*, i.e. a suitable combination of anonymity and accountability (Chaum, 1981). In particular, there are mechanisms to securely transfer signatures (expressing authorization, called credentials) between different pseudonyms of the same party (Chaum, 1985, 1990, 1992). This is called *transferring signatures between pseudonyms.*

When *pseudonyms* are used during accountable value exchange, there are a number of possibilities for the tasks of the integrated third party:

- Identification of the user in event of fraud (pseudonyms are certified and the certification authority knows real identities), i.e. privacy of pseudonymous parties cannot be guaranteed.
- Mandatory deposit of payment with an active trustee to prevent fraud in spite of completely anonymous pseudonyms, i.e. privacy of the pseudonymous parties can be guaranteed.

Multilateral Technologies

Multilateral technologies can only be used if a large number of independent parties cooperate

Multilateral technologies can only be used if a large number of independent parties cooperate. This means that coordination and possibly negotiation are needed on a large scale. Important multilateral technologies for multilateral security are:

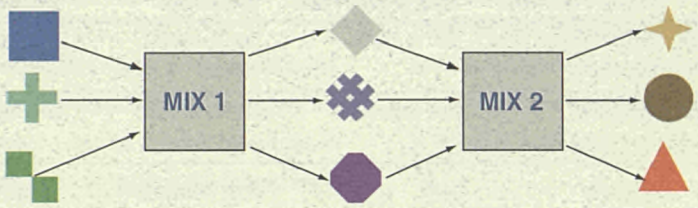
- *Tools to negotiate* multilateral protection goals and security mechanisms, e.g. for anonymity and unobservability.
- Mechanisms to provide *anonymity*, *unobservability*, and *unlinkability* with regard to
  - communications, i.e. protect who communicates when to whom and from where to where (Chaum, 1981, 1985, Pfitzmann, 1987, Cooper, 1995, Federrath, 1996, Jerichow, 1998, Reiter, 1999, Goldschlag , 1999) (See Fig. 3).
  - payments, i.e. protect who pays what amount to whom and when (Chaum, 1989, Asokan, 1997) and
  - value exchange, i.e. protect electronic shopping from observation (Bürk, 1990, Asokan, 1997).

All the above without compromising integrity, availability, or accountability.

Evaluation of maturity and effectiveness

Table 1 gives our evaluation of the maturity and effectiveness of the security technologies mentio-

Figure 3. Anonymity, unobservability, and unlinkability for communication



Functions of each MIX:
- batches
- discards repeats
- changes encoding (descryption)
- changes order

hides relation between in- and outgoing messages

MIXes can be used protect
- e-mail and Web-access. e.g. Onion Routing, and
- mobile communications

Together, all MIXes used can provably trace messages

ned in the previous sections. Their sequence in the table is mainly bottom-up, i.e. a technology for security placed in a particular row is required before a technology listed below can be effective. In some places, examples are given after a semicolon.

As can be seen, the weakest link in the security chain today is the user device, in particular its physical protection and operating system. Much has to be done to improve both.

Obviously, security evaluation of ICT and integration of security technologies are the challenges for research that have the greatest impact on ICT security.

Approaches to preventing cyber-crime and their side effects

Many of the approaches to preventing or prosecuting cyber-crime that have been discussed implicitly or explicitly aim at reducing ICT security in order to enable access by law enforcement agencies. Most of these mechanisms are based on the implementation of backdoors and loopholes (STOA, 2000), e.g. by integrating Trojan Horses in operating systems or by requiring encryption systems with key escrow or key recovery. However, it is likely that such backdoors and loopholes will be used by criminals as well as by authorized law enforcement agencies (Abelson, 1998). Moreover, such an approach is likely to be an obstacle to international trade in ICTs as no country would be able to trust ICT imported from abroad because of the risk that its security has been deliberately compromised.

Fundamental rights to privacy and anonymity –the default value in the offline world– run counter to the obligation upon the user to leave (authentic) data trails while using the Internet. On the other hand, demanding that providers log all traffic data and store it for a long time, not only jeopardizes privacy through the potential misuses of this information, but is heavily disproportionate: Anybody can render these logs completely useless by using encryption or strong steganographic tools and mechanisms for anonymity hosted in countries out-of-reach of domestic law enforcement, but well connected to the Internet and therefore well within reach both for privacy-conscious citizens and criminals. The real threat to cyber-crime prevention

The weakest link in the security chain today is the user device, in particular its physical protection and operating system

Fundamental rights to privacy and anonymity run counter to the obligation upon the user to leave (authentic) data trails while using the Internet

Table 1. Maturity and effectiveness of security technologies

	state of public research	demonstrators and prototypes	available products	products fielded on a large scale
physical protection	hardly any respectable publications	hard to assess	hard to assess; Me-chip	very poor; chipcards
security evaluation of ICT	acceptable	hard to assess	hard to assess	hard to assess
security in operating systems	very good	good	poor; Windows NT Windows 2000, Linux, Mac OS X	very poor; Windows 98, Windows ME, Windows CE, Mac OS 9.x
cryptography	very good	good	good; PGP 2.6.x	acceptable; PGP 5.x, PGP 6.x
steganography	good	acceptable	poor	very poor
public-key infrastructure	very good	good	hard to assess	
security gateways	good	acceptable		
mechanisms for anonymity, unobservability, and unlinkability	very good	good	acceptable; Onion Routing, Freedom	poor; proxies
digital pseudonyms	very good	good	good; PGP 2.6.x	acceptable; PGP 5.x, PGP 6.x
transferring signatures between pseudonyms	good			
tools to help even inexperienced users to formulate and negotiate	good	acceptable		
integration of these technologies	acceptable	poor	poor	very poor

Measures which are perceived to involve spying indiscriminately on the public in the name of detecting criminal activities run the risk of creating solidarity between privacy-conscious citizens and potential criminals

and prosecution is that such disproportionate measures tend to create solidarity between privacy conscious citizens and potential criminals. All experience with fighting organized crime shows that this kind of solidarity is one of the most serious obstacles to success. Phil Zimmermann stated this quite concisely: "If privacy is outlawed, only outlaws will have privacy" (see Note 1). Taking this approach to policing cyberspace may, therefore, prove counterproductive.

As may be seen in Table 1, the state of public research into security technologies is quite advanced in most cases. An effort is needed, however, to implement these technologies in standard products so as to enable all users of open networks to benefit from them. Less effort is required to protect communication within a closed group of educated users. This means criminal organizations can create and use their own set of security tools as well as any other closed user group, thus making, restrictions

on cryptography easy to circumvent by precisely those groups whose activities they are intended to curtail (Franz, 1996).

From this viewpoint it seems to be logical to discuss active attacks by law enforcement agencies, e.g. denial-of-service attacks, unleashing viruses, or modifying content on computer hard disks of incriminated subjects (see Note 2, Walsh , 1996).These info-war techniques might effectively work according to the saying "the end justifies the means", but such "licences to hack" are not only dubious from the legal point of view, but the authenticity of evidence investigated by attacks that manipulate data is highly doubtful as well.

Thus, we have to be aware of the fact that cyber-crime prevention is not only in tension with privacy, but with ICT security as well:

- Many tools needed to test security can also be used for hacking insecure systems.
- It will be possible to use backdoors and loopholes to manipulate traces (by either authorized or unauthorized parties) as well as surveillance by authorized parties.

On the other hand, security technologies provide the tools to prevent those types of cyber-crime which are specific to computer networks: Public research and development in this area will lead to more secure systems enabling users to protect themselves.

Conclusions

To conclude, the current state of ICT security may be summed up as follows:

- ICT security is generally extremely weak, and to try to improve it effectively is an ambitious undertaking.
- All backdoors and loopholes installed on behalf of law-enforcement agencies will be quickly exploited by criminals i.e. these cyber-crime prosecution technologies are, therefore, cyber-crime enabling technologies.
- Whatever steps are taken, astute criminals will come up with effective techniques to conceal
  - what they store and what and with whom they communicate from where to where, or even
  - whether they store and communicate at all.

Thus, if legal restrictions are placed on the privacy permitted by ICT, only criminals will enjoy unrestricted privacy.

In particular, it is crucial to ensure that efforts to combat cyber-crime must not slow the improvement of ICT security or weaken it even further (See note 3). In the current situation, law enforcement agencies should only be allowed and enabled to exploit security weaknesses of ICTs still present under tightly controlled circumstances. They should not be permitted to force the implementation of additional weaknesses.

In the long run, the security weaknesses of ICT should diminish and all users should be empowered to decide on their own level of security and privacy. Law enforcement agencies should use technologies which allow effective supervision of individuals and small groups, but which do not scale to allow mass surveillance of those who do not protect themselves adequately. These technologies for individual surveillance lie outside the ICT infrastructures. Mass surveillance may seem the easiest option for law enforcers, but what is important is to implement what is effective and not what is easiest. Moreover, democracy cannot be protected by building an Orwellian ICT infrastructure.

All the same, we need an open discussion about cyber-crime prevention and prosecution in which law enforcement agencies, privacy pressure groups, the ICT industry, users and politicians take part before regulating the topic.

Loopholes and backdoors left in systems to allow access to law enforcers are likely to be rapidly exploited by criminals

Looking for a balance, we may conclude that there is no way to achieve effective surveillance or curtailment of criminal activities by weakening ICT security. Instead, security tools have to be improved in order to provide better protection for users, i.e. to protect them against cyber-crime. At all events, technology alone cannot prevent all kinds of criminal action. There is a need for policy action instead of calls for police action (see note 4). We have to keep in mind that it is not just a matter of coping with potential economic losses, which we might even be insured against. Instead, we want to defend our democratic society in its entirety against damage. Thus, privacy and security must not be put at stake.

Keywords

cyber-crime prevention, cyber-crime prosecution, multilateral security, security, privacy, technology

Notes

1. Phil Zimmermann: Why do you need PGP? June 5, 1991; **http://www.pgpi.org/doc/whypgp/en/**
2. E.g. with the software "D.I.R.T. – Data Interception by Remote Transmission" from the US company Codex Data Systems (**http://www.codexdatasystems.com/menu.html**), further information about D.I.R.T. is available at Cryptome, **http://cryptome.org/dirty-secrets2.htm**
3. Similarly, in (EC, 2001) "The legitimate concerns about cyber-crime necessitate effective law enforcement investigations. However these legal concerns should not create solutions where legal requirements lead to weakening the security of communication and information systems."
4. Personal communication with Dieter Klumpp, Managing Director Alcatel SEL Foundation for Communication Research, Stuttgart, 2001; similarly in his speech "Electronic Government und Bürgernetze", Deutscher Städtetag, Stuttgart, April 26, 2001.

References

- Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B. *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, Final Report*, May 27, 1997, updated: June 8, 1998; **http://www.cdt.org/crypto/risks98/**
- Asokan, N., Janson, P. A., Steiner, M., Waidner, M. *The State of the Art in Electronic Payment Systems*; Computer 30/9, 1997, pp. 28-35; **http://www.semper.org/sirene/publ/AJSW_97PayOver.IEEE.pdf**
- Anderson, R., Needham, R., Shamir, A. *The Steganographic File System; Information Hiding*, 2nd Workshop, Portland, Oregon, LNCS 1525, Springer, Berlin 1998, 73-82; **http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/sfs3.pdf**
- Asokan, N., Schunter, M., Waidner, M.*Optimistic Protocols for Fair Exchange*; 4th ACM Conference on Computer and Communications Security, Zurich, April 1997, pp. 6-17; earlier version: **http://www.semper.org/sirene/publ/AsSW_97FairX.CCS.ps.gz**
- Bürk, H., Pfitzmann, A. *Value Exchange Systems Enabling Security and Unobservability*, Computers & Security 9/8, 1990, pp. 715-721; **http://www.semper.org/sirene/publ/BuePf_90.ps.gz**
- Chaum, D. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*; Communications of the ACM 24/2, 1981, pp. 84-88; e.g. at **http://world.std.com/~franl/crypto/chaum-acm-1981.html**
- Chaum, D. *Security without Identification: Transaction Systems to make Big Brother Obsolete*; Communications of the ACM 28/10, 1985, pp. 1030-1044; **http://www.chaum.com/articles/Security_Wthout_Identification.htm**
- Chaum, D. *Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability*; SMART CARD 2000: The Future of IC Cards, Proc. of the IFIP WG 11.6 Intern. Conference; Laxenburg (Austria), 1987, North-Holland, Amsterdam 1989, pp. 69-93.
- Chaum, D. *Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms*; Auscrypt '90, LNCS 453, Springer, Berlin 1990, pp. 246-264.

- Chaum, D. *Achieving Electronic Privacy*; Scientific American, August 1992, pp. 96-101; **http://www.chaum.com/articles/Achieving_Electronic_Privacy.htm**
- Cooper, D. A., Birman, K. P. *Preserving Privacy in a Network of Mobile Computers*; 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, pp. 26-38; **http://www.it.kth.se/edu/gru/Fingerinfo/telesys.finger/VT95/Mobile.VT95/Papers/dcooper-security.ps**
- European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach*; June 6, 2001; **http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_en.pdf**
- Federrath, H., Jerichow, A., Pfitzmann, A.: *Mixes in mobile communication systems: Location management with privacy; Information Hiding*, 1st Workshop, Cambridge, UK, LNCS 1174, Springer, Berlin 1996, pp. 121-135; **http://www.semper.org/sirene/publ/FeJP1_96MobileMIX.ps.gz**
- Franz, E., Jerichow, A., Möller, S., Pfitzmann, A., Stierand, I. *Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best*; Information Hiding, LNCS 1174, Springer, Berlin 1996, 7-21; **http://www.semper.org/sirene/publ/FJMP_96Stego.ps.gz**
- Goldschlag, D., Reed, M., Syverson, P. *Onion Routing for Anonymous and Private Internet Connections*; Communications of the ACM 42/2, 1999, pp. 39-41; **http://www.onion-router.net/Publications/CACM-1999.pdf**
- Jerichow, A., Müller, J., Pfitzmann, A., Pfitzmann, B., Waidner, M. *Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol*, IEEE Journal on Selected Areas in Communications 16/4 May 1998, pp. 495-509.
- Pfitzmann, A. *Multilateral Security: Enabling Technologies and Their Evaluation*, in: R. Wilhelm (Ed.): Informatics – 10 Years Back, 10 Years Ahead, LNCS 2000, Springer, Berlin 2001, pp. 50-62.
- Pfitzmann, A., Waidner, M. *Networks without user observability*; Computers & Security 6/2, 1987, pp. 158-166.
- Pfitzmann, A., Pfitzmann, B., Schunter, M., Waidner, M. *Trustworthy User Devices*; in: G. Müller, K. Rannenberg (Eds.): Multilateral Security in Communications, Addison-Wesley, Munich 1999, pp. 137-156.
- Pfitzmann, A., Schill, A., Westfeld, A., Wicke, G., Wolf, G., Zöllner, J. *A Java-based distributed platform for multilateral security*; IFIP/GI Working Conference "Trends in Electronic Commerce", Hamburg, LNCS 1402, Springer, Berlin 1998, pp. 52-64; **http://www.semper.org/sirene/publ/PSWW_98.pdf**
- Reiter, M. K., Rubin, A.D. *Anonymous Web Transactions with Crowds*; Communications of the ACM 42/2, 1999, pp. 32-38.
- STOA (Scientific and Technological Options Assessment), European Parliament: *Development of surveillance technology and risk of abuse of economic information*, 1998-2000; **http://www.europarl.eu.int/stoa/publi/pop-up_en.htm**
- Walsh, G. *Review of Policy relating to Encryption Technologies* (Walsh-Report), prepared in 1996 by the Australian Attorney-General's Department, different parts publicly released 1997-1999; **http://www.efa.org.au/Issues/Crypto/Walsh/** (website of Electronic Frontiers Australia).
- Wolf, G., Pfitzmann, A. *Properties of protection goals and their integration into a user interface*; Computer Networks 32, 2000, pp. 685-699.

Contacts

Andreas Pfitzmann, Dresden University of Technology, Department of Computer Science, Institute for System Architecture
Tel.: +49 351 463 82 77, fax: +49 351 463 82 55, e-mail: **pfitza@inf.tu-dresden.de**
Marit Köhntopp, Independent Centre for Privacy Protection
(Unabhängiges Landeszentrum für Datenschutz) Schleswig-Holstein
E-mail: **marit@koehntopp.de**
Laurent Beslay, IPTS
Tel.: +34 954 488 206, fax: +34 954 488 208, e-mail: **laurent.beslay@jrc.es**

About the authors

Andreas Pfitzmann is a professor of computer science at Dresden University of Technology. His research interests include privacy and multilateral security, mainly in communication networks, mobile computing, and distributed applications. He has authored or coauthored about 70 papers in these fields. He received diploma and doctoral degrees in computer science from the University of Karlsruhe. He is a member of ACM, IEEE, and GI, where he serves as chairman of the Special Interest Group on Dependable IT-Systems.

Marit Köhntopp received her diploma in computer science from the University of Kiel, Germany. She is head of the "Privacy Enhancing Technologies (PET)" Section at the State Privacy Commission of Schleswig-Holstein. Her research interests include privacy and multilateral security, especially in the Internet, and all kinds of privacy enhancing technologies from both the technological and the legal perspectives.

Crime and Abuse in e-Business

Neil Mitchison and Robin Urry, *Institute for Protection and Security of the Citizen (IPSC), JRC*

Issue: The criminal or abusive misuse of information and communications technology is a problem of growing significance in the information society. E-Business, in particular, will require user confidence if it is to grow.

Relevance: Common reporting procedures for computer crime incidents and standards of evidence are an important part of the response to cyber-crime. Policy initiatives in this area, however, need to be flexible enough to respond to the rapid evolution of both ICT technology and its exploitation by criminal elements.

The computing industry has long been concerned with security issues, particularly in the financial sector, but the spread of the Internet has given many of these concerns a much higher public profile

There is a widespread belief that cyber-crime is substantially under-reported, whether through ignorance, lack of faith in response measures, or a desire to avoid bad publicity

The importance of cyber-crime

Few who work in the field of electronic communications and transactions are in any doubt as to the importance of cyber-crime. Combating computer-based crime –in particular that internal to a company– has long been a concern of developers, implementers and administrators of computer systems, especially in the financial sector; although it sometimes seems as if the world of politics and the media has only just become aware of the possibilities of cyber-crime, and is now insisting on an instant, and totally effective, response. The vulnerabilities which have led to this awareness are real enough: among them is the very nature of e-business, which requires the automation of various types of security procedures and "reality checks"; the ease with which a vulnerability, once identified, can be exploited from anywhere in the world; and the sheer quantity of traffic over the Internet, which makes any sort of monitoring difficult. Some new tools have had to be developed to cope with these specific vulnerabilities; but many computer security procedures and standards had already been developed long before the Internet arrived.

It is extremely difficult to put hard figures on the incidence of cyber-crime, whether Internet-based or more "traditional", but it certainly exists: many different types of incident and attack have been identified, and some users have reported very large numbers of attempted intrusions, sometimes successful. There is a widespread belief among those dealing with the subject that cyber-crime is substantially under-reported, whether through ignorance, lack of faith in response measures, or a desire to avoid bad publicity.

Whatever the incidence of cyber-crime, there is little doubt about the widespread vulnerabilities; and it is reasonable to suggest that public policy should encourage protection and countermeasures without waiting for proof that these vulnerabilities

are being widely exploited. Indeed, the experience of law enforcement in other areas has shown that where there are opportunities for crime, criminals soon arrive to exploit them.

A further consequence of cyber-crime –or perhaps more specifically, of the perception of cyber-crime– is its effect on confidence. Again hard figures are difficult to obtain, but it appears that lack of confidence in protection and response measures against cyber-crime is a significant brake on the development of electronic business, particular "B2C" or "Business to Consumer" transactions. Before a consumer starts electronic commerce, he will have some "confidence requirements". These might include:

- that the business is honest
- that the business is financially sound
- that redress in the case of dispute is a practical option
- that there is reasonable protection against criminals intervening in the transaction.

Various mechanisms are under development to help consumers to acquire this confidence in appropriate cases (see **http://econfidence.jrc.it/**), but there is still much to be done. Recent incidents have attracted much media attention, and this has certainly had the positive effect of alerting system developers and e-commerce providers to the vulnerabilities of their systems; but in the absence of reliable figures on cyber-crime it is hard to evaluate the effect of media attention on the general public's perception. Thus, although it may have corrected over-confidence, it may also have led to excessive caution.

Taxonomy

One of the first questions to be addressed is the definition and classification of "cyber-crime". This can be interpreted as meaning any criminal or abusive activity involving computers, but that definition is too wide to be of use technically. The first and most fundamental distinction is that between using a computer as a tool in a crime and the computer system (or its data) being the target of the crime. The focus here is on the latter[1].

When we come to ask which activities should be considered, it is clearly unsatisfactory to use a definition based on criminal or civil law; these differ from one jurisdiction to another, are in rapid evolution in several countries, and leave considerable "grey areas" as to what is or is not covered in the event of activities spanning several jurisdictions. Therefore, the definition used here is based on what administrators and users of computer systems find unacceptable rather than any strictly legal definition.

Of course the failure to use a legal definition could lead to problems, in particular not knowing whether a particular activity is or is not covered. However, from a technical point of view the legal status of a particular abusive activity is usually of minor interest; what is important is to know what is going on, and detect and stop what is unacceptable. The exception perhaps comes in the area of the reaction to incidents, where the possibility of legal proceedings may constrain severely the process of gathering evidence; in that case it may be appropriate to take quite different actions against "antisocial" activities and "criminal" ones.

If the external boundaries of the domain covered are somewhat fuzzy, the same is true for some of its internal distinctions. Various taxonomies have been proposed for cyber-crime incidents, but we found none of them to be fully convincing and comprehensive[2]. There are three fundamental approaches to such a taxonomy: one based on the technical actions carried out, the second based on the intent of the perpetrator, and the third based on the effects (real or hypothetical) of the actions. But none of these is fully defined,

A lack of confidence in protection and response measures against cyber-crime would appear to be a significant brake on the development of electronic business, particular "B2C" or "Business to Consumer" transactions

Although cyber-crime broadly includes any criminal or abusive activity involving ICTs, a fundamental distinction exists between using a computer as a tool in the perpetration of a crime, or making it the target

The three main approaches to a taxonomy of cyber-crime are based on the technical actions carried out, the intent of the perpetrator, and the effects of the actions

Security needs to be understood as a process not a product. Software tools are not enough in themselves, but need correct installation and use, and continuous monitoring

nor fully satisfactory. Thus if we use the technical taxonomy of actions for the top level, we would want to distinguish between:

- gaining access to data
- modifying data
- attacking computer functioning
- attacking network functioning

However, this top-level distinction groups together very different activities. "Gaining access to data" means different things if the data concerned represents:

- the root administrator's password
- a file of credit card numbers
- a pop song

Moreover, an individual incident is likely to involve more than one of these activities - having found the root administrator's password, what is the cracker going to do next?

Similarly, however important the attacker's intent may be in legal proceedings, it does not yield a satisfactory basis for a technical classification of cyber-crime incidents: it is often not known at the time of an incident, and can only be established with the aid of external information. Distinguishing by the effects –real or hypothetical– of the actions is tempting in some instances, and is indeed standard industry practice. However it leaves a lot to be desired as a formal analytic tool, in particular because the possible effects of any sort of "cracking" attack are almost unlimited.

Although a fully developed taxonomy does not appear to be within reach at present, it is possible to identify the five main areas of concern listed below:

- Fraudulent transactions in e-business (whether from provider or client)
- Identity theft and "passing off"
- Credit card number and similar thefts (can be seen as a form of identity theft)
- Theft of IPR
- Denial of service and internet attacks.

Prevention and Detection

In the areas of prevention and detection of cyber-crime, there is a wide range of commercially available software products, as well as some more specialised toolkits for particular markets[3].

Two areas stand out as needing further attention. Firstly "security is a process not a product": software tools are not enough in themselves, they must be correctly installed and used, and continuous monitoring is essential. Secondly –and this is of course related to the first point– there is still a widespread need for training concerning awareness and basic precautions (among staff and clients), the selection and use of particular prevention tools, and whether and when to call in expert help.

In some countries and industry sectors across Europe, a market appears to be developing for centralized monitoring services to help detect cyber-crime in real time. Monitoring transactions to detect cyber crime requires specialist staff and equipment, and only the very largest companies are likely to have the resources to carry this out effectively in-house. Many of the large business consultancies now offer computer forensic services to their clients for internal security and incident investigation.

The growth of CERTs (Computer Emergency Response Teams) over the last few years has added significantly to the armoury available to deal with cyber-crime incidents. However the provision of CERT facilities is still fragmentary, apparently at least in part owing to a lack of awareness among potential clients. The European Commission has recently called for a strengthening of the CERTs and improving cooperation among them[4].

Response

When an incident has happened, there are two –sometimes conflicting– needs: the integrity of the system has to be restored, and the incident has to be investigated[5]. This means collecting, preserving, organizing, and subsequently presenting the evidence of what happened. If this evidence is to be presented to the system administrators to help them protect their system better, a very informal approach may be acceptable; but as soon as there is any possibility of the investigation going further, it is necessary to ensure that the evidence produced meets the requirements of the authorities involved. These authorities could range from internal company disciplinary procedures, through mediation and out-of-court settlement, to civil or criminal courts. Each of these bodies may have its own rules on the admissibility of evidence, and it is important that initial investigations of suspected incidents do not contaminate the electronic evidence so that it cannot be used.

There are many "forensic" tools available on the market for investigation of computer incidents. With the aid of these, log files can be studied and interrogated; deleted and discarded data can be salvaged; the crucial points in a complex system can be identified; and the events which occurred in the incident can be reconstructed. Some of these tools also help in the construction of a coherent chain of evidence. However, there is need for further work to produce an overall methodology to ensure that the chain of evidence is fully guaranteed; and even when that is available, it will have to be integrated with the target system. Ultimately, the aim must be not merely to be able to demonstrate "this was the state of the computer system and data when we started investigations", but "this is the proof of what had happened previously".

If such an investigation goes to court –especially a criminal court with its high standards of proof– in order to fully satisfy the court of the accuracy of the statements made, it may be necessary to produce source files for the forensic tools used, and even for the operating system and software. This is a challenge which the industry has not fully faced up to yet, and it may be that over time this requirement leads to much more widespread use of open source software, not just for computer forensic tools, but also for e-business applications and servers running them.

Standards

The question of European or worldwide standards often comes up in this context, but two particular areas stand out: reporting procedures and evidence analysis standards.

It is simply not possible today to determine precisely the incidence of cyber-crime. Figures can be collected here and there, but it is not clear what they mean and how one can be compared with another. The only figures which have some element of comparability are figures for financial losses (always assuming (a) that the companies concerned know how much they have lost, and (b) that they report it truthfully). While common reporting procedures for computer crime incidents would not resolve all the difficulties of data - in particular the problem of under-reporting - they could at least give some sort of basis for comparing one sector, one country, one time, or one activity with another. The US model is potentially instructive; it comprises an Internet Fraud Complaints Centre and a National White Collar Crime Centre which provide useful clearing-houses for incident reporting, thereby offering a certain amount of consistency across different sectors and different types of incident.

As for evidence analysis standards, there is a need for the development, in parallel with integrated evidence collecting systems, of agreed standards for the collection and analysis of log data and other similar files. These standards should ensure

After an incident has taken place, the need to restore the system quickly may conflict with the need to collect, preserve and organize evidence which may be required in criminal proceedings

Common reporting procedures would clearly not resolve all the difficulties of data, such as under-reporting, but they would give some sort of basis for comparing countries, sectors, or activities, etc.

that the investigators also respect the requirements of European Data Protection laws, to protect the privacy of innocent parties during investigations. In the absence of a well-defined approach respecting data protection and privacy, then either incidents will not be investigated or innocent parties' right to privacy will be violated.

Conclusions

At the end of 2000, IPSC staff, along with a team from other European research organizations, launched a study on the fight against criminal and abusive activities ("cyber-crime") affecting e-business. The study aims at establishing a technical "state of the art", in other words to define the present situation and expected evolution of tools and procedures to combat cyber-crime. The study group identified three principal technical areas of concern: the prevention of cyber-crime, the detection of cyber-crime, and response to incidents of cyber-crime. However it soon became clear that a further area had to be addressed, namely the development of standards.

At the time of writing (June 2001), the study's report is still in draft form. The preliminary work of the study group has highlighted areas where further work is needed on the technical aspects of the prevention, detection, and response to cyber-crime. This is not all; policy initiatives, in terms of both legal and administrative actions, are also needed, and are indeed under way in many countries of the European Union and at EU level. However, these policy initiatives will take time, and the world of computers –and of criminals–moves fast. There is a lot that can be done by the developers, providers, and users of e-commerce systems to provide better protection against cyber-crime.

About the authors

Neil Mitchison has a degree in mathematics from Cambridge (UK), and spent ten years as a computer consultant working on research in artificial intelligence and the development of financial reporting systems for large companies. He joined the Joint Research Centre in 1988, where he has worked on real-time monitoring systems, safety-critical systems, and on challenges of safety and security in both the on-line and off-line environments.

Robin Urry qualified as a mechanical engineer, and subsequently also studied politics and business administration. He has worked for some 20 years in the IT industry, 10 of them as a senior manager with Digital and 4 with Scottish Enterprise working on e-commerce development. He has been a Special Constable for 6 years. He is currently Director of Cybersecure Scotland Ltd., and is spending a year as Visiting Scientist at the Joint Research Centre.

Keywords

cyber-crime, taxonomy, prevention and detection, data reporting standards

Notes

1. This is not to exclude the possibility of some "spill-over", in particular in the domain of response and evidence gathering: a reliable system for gathering and preserving electronic evidence could be useful in investigating and judging many sorts of crime which use computers as a tool.
2. The only well-developed international effort at a legally-defined taxonomy is the Council of Europe's draft convention on cyber-crime - see **http://conventions.coe.int/treaty/EN/projets/cybercrime25.htm** for the 25th draft. However that is deliberately limited in its scope.
3. The study group is evaluating the core toolkits against a general threat analysis, with a view to developing a common security model. This work is ongoing.
4. **http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_en.pdf**
5. There is some suggestion that a further reason for the under-reporting of cyber-crime incidents is that commercial pressure to get the system running again takes priority over incident investigation.

Contacts

Robin Urry, JRC
Tel.: +39 (0332) 78 92 63, fax: +39 (0332) 78 95 76, e-mail: **robin.urry@jrc.it**
Neil Mitchison, JRC
Tel: +39 (0332) 78 53 25, fax: +39 (0332) 78 90 07, e-mail: **neil.mitchison@jrc.it**
Laurent Beslay, IPTS
Tel.: +34 954 488 206, fax: +34 954 488 208, e-mail: **laurent.beslay@jrc.es**

The Fight against Cyber-Crime: The Need for Special Training on Digital Evidence

Eric Freyssinet, *Gendarmerie Nationale, France*

Issue: Combating cyber-crime is one of the greatest challenges facing society today, and efforts to tackle it involve law enforcement authorities, industry and the public. The dangers at stake have been widely pointed out by the media, and underlined in recent official statements, such as the European Commission communication of 2000 on a safer information society – COM (2000) 890. Digital evidence is key to the detection and prosecution of the perpetrators of both cyber crime and an increasing portion of other categories of crime.

Relevance: Computers, the Internet and a wide variety of digital devices have now become a familiar part of citizens' everyday lives. They are also familiar to criminals. Fighting crime today means taking into account all possible sources of information or evidence, and this increasingly includes digital evidence. When fighting high-technology crime this kind of evidence is even more necessary. Law enforcement authorities, lawyers and judges need to become familiar with these new tools, which means proper training is necessary at all levels.

Introduction

Recently, the issue of training in the use and gathering of digital evidence[1] has been raised forcibly at the highest levels. Thus, in their Moscow Communiqué of December 10th 1997, the Justice and Interior Ministers of the G8 countries declared "III. Law enforcement personnel must be trained and equipped to address high-tech crimes", as the Third Principle of combating high-tech crime.

The emphasis placed on this need arises out of a realization that high-tech crime, or information technology crime, poses a very serious threat to our economies and the everyday lives of our citizens. More recently, the IOCE (International Organization on Computer Evidence) has put forward a number of principles guiding the management of digital evidence and procedures to be followed when using it. The third of these reads: *"When it is necessary for a person to access original digital evidence, that person should be trained for the purpose."*

There are a number of reasons for this widespread concern. Firstly, information technologies now pervade all aspects of society. Digital telephones, computers, the Internet or on-board guidance systems for cars are no longer toys for a privileged

High-tech crime, or information technology crime, poses a very serious threat to our economies and the everyday lives of our citizens

few or for technology buffs. Secondly, these new tools manipulate information, and this information can be useful in any investigation, whether it be specific to crimes against computers or digital devices, or simply involving them. Thirdly, because it is important for the proper functioning of our legal system, and to protect the rights of all parties, to deal with digital evidence with the same care as any other piece of potential evidence. Finally, in a networked environment, where a crime occurs in one country, and both the victim and the suspect live in other countries, it is essential that the same level of expertise is reached in all those jurisdictions to ensure investigation data or digital evidence can be exchanged effectively when necessary.

Where a crime occurs in one country, and both the victim and the suspect live in other countries, it is essential that the same level of expertise is reached in all the jurisdictions involved in order for digital evidence to be exchanged effectively

Training all the actors at all levels

There are difficulties at all levels when dealing with digital evidence. Incorrect handling of a computer, for example, may alter potential evidence. Managing a police operation inadequately might lead to ineffective use of the available digital evidence. And, a failure to understand the value of digital evidence might also mislead the decisions of a jury. Thus, all the actors involved need proper training.

Every police officer knows that when arriving on a crime scene it is his responsibility as a first responder to do his best to preserve the evidence. However, at present the police are often unaware of the value of digital evidence or the way in which it should be handled

Nowadays, every police officer knows that when arriving on a crime scene it is his responsibility as a first responder to do his best to preserve the evidence, as well as to help the victims and identify possible witnesses. At present, the police are often unaware of the value of digital evidence or the way in which it should be handled. Simple techniques for first responders have been identified. Various guides are being developed by different police agencies in the world, Interpol working parties (**http://www.interpol.int/**) **and the IOCE** (**http://www.ioce.org/**). These need to be exchanged, promoted and distributed.

Once collected, material holding digital evidence is passed on to a specialized investigator, who might want to have quick access to the information stored to assess its value to the investigation. Working in laboratory conditions takes a certain amount of time and might be inappropriate to the needs of the investigation if speed is of the essence. In some cases it is possible to read information stored on digital media using simple means without altering the original evidence. It is also important that the investigator understands quickly the potential usefulness of digital information to his investigation so as to be able to decide whether it is necessary to call in experts. Making decisions of this kind calls for a certain degree of understanding of the subject, thus creating a need for the relevant training. To this end, guidelines have been developed, and training packages are being set up by groups of specialists. They should be used and implemented at national level.

Obviously, forensic laboratory specialists need to be properly equipped and trained. In particular this training needs to be regularly updated to keep up with rapidly changing technology. Working groups of specialists have been set up worldwide to study this issue. For instance in Europe within ENFSI (European Network of Forensic Science Institutes) and its FIT working group (**http://www.enfsi.org/**).

Eventually, the evidence has to be explained to a judge or a prosecutor. For example, IP addresses or dates of file accesses are details that will be addressed in a police or forensic laboratory report. Judges and lawyers must understand the significance of the information and the meaning of the technical details to be able to judge or present the case fairly. However, it would not be realistic to expect legal specialists to also become experts in IT, so proper training must be devised for those people who do not have a technical background but need to make decisions based on technical information.

The issue is similar for law enforcement decision-makers. They need to understand the specifi-

cities of digital evidence so as to be in a position to provide their people with the proper training and tools, and to take the operational decisions appropriate to their area of competence. This could mean, for instance, organizing the storage of dozens of computers seized during a large police operation.

These training needs exist in all countries and are particularly important when a number of different countries are involved in a criminal case. Where criminal investigations cross borders it is necessary for the evidence collected in one country to be legally recognized and properly interpreted in the country where the crime is prosecuted. Clearly, international standards are needed if this is to be achieved.

New tools for training

A wide range of training needs have been identified. These needs should be addressed in law enforcement or justice academies, which should be appropriately equipped with computerized training rooms. But the people in place also need to receive training and information and sending everybody back to the classroom might not always be the best solution. Moreover, this field is a quickly evolving one, making frequent updates essential. Simple guidelines need to be provided, and new types of training tools should also be considered.

When looking for information about new technologies, the first place to go is of course the Internet. Using the powerful resources of search engines to search for general documents, guides for beginners or precise technical white-papers should be everybody's first reaction. Internet services and facilities should be made readily available for technical experts, investigators, managers and judges.

To distribute modern training material, CD-ROMs or DVD-ROMs will progressively replace books or video-tapes. CD-ROMs are a lot less expensive to produce, easier to transport and distribute, and can contain a large amount of information. An international training CD-ROM for first responders will be launched this year, coordinated by Interpol and funded by a private sector initiative. But, when on a crime scene, the investigator will still need a compact checklist, and traditional pen and paper may often be the most appropriate solution, even if the more up-to-date investigators may wish to download those checklists onto their PDAs (personal digital assistants).

Digital training tools could be more interactive if distributed in a connected – but secure – environment, such as an Intranet. This could host regularly updated technical databases, online courses that could be adapted easily to the latest technologies or a live discussion (or *chat*) with specialists who are often otherwise difficult to reach. In our e-Europe environment, all ministers and police agencies are gradually being equipped with such a network. In France for instance, the Gendarmerie Nationale will have deployed its Intranet in all its 3600 local units by 2003, and it is already available through over 100 access points, which allow field trials to be scheduled very quickly.

A secure environment can be set up on an Internet server, providing similar services to an intranet (see Box 1). Interpol and ENFSI are moving in this direction as a means of providing training material and technical databases to police and forensic laboratory specialists all over Europe and the world.

All these new tools are urgently needed, and will help provide an efficient, inexpensive and rapid solution to providing decentralized training.

Crime prevention

The responsibility of law enforcement goes beyond the needs of law enforcers themselves. The general public and the management of industry

Investigators need to have sufficient understanding of the issues regarding digital information to know when they should call in experts. Training is therefore essential

Standards for the gathering, preservation and validity of digital evidence need to be harmonized across countries if cross-border criminal investigations are to be effective

Users and potential users of the Internet need to be properly informed about the risks of their encountering illegal and offensive content and to be aware of channels through which to report it

must be informed in order to better prevent and report crime involving information technologies.

Box 1. The Gendarmerie Nationale Intranet – France

Like any other major institution in France, the Gendarmerie Nationale, the second-largest national police force in France, with 96,000 people, is using a large secure communications system. In view of the new possibilities offered by Internet technologies, in 1998 the Gendarmerie decided to set up its own specific Intranet.

This Intranet originally contained a series of web pages, a directory and a database of all legal texts in force (over 9000 documents relating to the operation of the Gendarmerie Nationale which had traditionally been stored on paper and were put on CD-ROMs in the 1990s).

A number of other major applications, mainly in the form of centralized databases, have been identified and are currently being transferred on to the Intranet. Training is another application which is being developed. As a starting point, standard training documents are being converted into web documents, but more interactive features will eventually be developed, such as online classrooms.

The advantages of the Intranet as a training tool include its cost effectiveness (less paper to be mailed all over the country), ease of upgrading and interactivity.

As an open environment the Internet creates new dangers for children as well as for corporate networks. Parents, users, security specialists, and managers must be informed about the dangers, and they must also have the possibility of using properly configured software and hardware to protect themselves, their loved ones or their corporate assets.

Informing the Internet-using public is an essential task. But the public must also be informed before going online, through more traditional mass media, in classrooms or when meeting law enforcement bodies. In Canada, for instance, the government has launched a specific programme called "Illegal and offensive content on the Internet" which consists of a 32 page booklet available both on and off the Internet. It also makes use of television and newspaper advertising to inform Internet users of harmful or illegal content on the Internet, ways adults can protect themselves and their children, and also the channels through which to report abuses.

Industry can also be a major partner in our fight against crime, or more simply in preventing the dangers brought by the use of information technologies. First, in developing and promoting the use of safer computer environments, e.g. better protected operating systems, secure electronic transactions; secondly, by implementing better IT security within their own organizations, including implementation of proper storage and manipulation of potential evidence of attacks against their systems; and, thirdly, by assisting law enforcement bodies in the process of informing the public. The INHOPE initiative, (partly funded by the European Union) which aims to inform the public and encourage the reporting of illegal content, is worth repeating in other domains. This could possibly be extended to informing witnesses of a crime how best to preserve and present digital evidence.

There is today an urgent need for the proper training of all actors – investigators, judges and managers – who will be dealing with digital evidence in criminal investigations, especially those involved in the fight against cyber-crime. This training must reach all our partners equally and in a standard way to guarantee the protection of all citizens in today's networked and open environment. Industry and the public are our partners in the prevention of those crimes or specific dangers. To achieve our goals we need to use new technologies so as to operate in a way that is faster, less expensive and more effective.

Keywords
information technology, cyber-crime, forensics, training, digital evidence

Note

1. For the purpose of this article, we shall define "digital evidence" as any material containing information in a binary format, that is the language of computers or micro-processors.

References

- Communication from the European Commission to the Council and the European Parliament, *Creating a safer information society by improving the security of information infrastructures and combating computer-related crime* (COM(2000)890) – **http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html**
- *Illegal and offensive content on the Internet – The Canadian strategy to promote safe, wise and responsible internet use* – **http://www.brancher.gc.ca/cyberwise/index.htm**
- INHOPE – The association of Internet hotline providers in Europe – **http://www.inhope.org/**

Contacts

Eric Freyssinet, Institut de recherche criminelle de la gendarmerie nationale
Tel.: +33 1 49 35 50 62, fax: +33 1 49 35 50 27, e-mail: **eric.freyssinet@enfsi.org**
Laurent Beslay, IPTS
Tel.: +34 954 488 206, fax: +34 954 488 208, e-mail: **laurent.beslay@jrc.es**

About the author

Eric Freyssinet, studied at the Ecole Polytechnique, Palaiseau (France) and the Gendarmerie nationale's school for commissioned officers. Since 1998 he has worked at the Information technology forensics department of the Institut de recherche criminelle de la gendarmerie nationale (forensic research institute), and has been head of this department since 1999. He is the chairman of the Forensic information technology working group of ENFSI (**www.enfsi.org**) and vice-chairman of Interpol's European working party on information technology crime.

Cyber-Security and the Future of Identity

Marc Bogdanowicz and Laurent Beslay, *IPTS*

Issue: Everyday communication and participation in the public sphere is tacitly underpinned by our shared understanding of the nature of identity, and our reliance on mechanisms of identification that enable us to trust information given by individuals we do not know personally. The processes central to the information society, such as digitization and remote interaction across communications networks, are placing existing models of identity and mechanisms for identification under increasing strain.

Relevance: Identification, authentication, privacy, and security of personal information are key issues for the information society. The misuse, either by individuals or organizations, of sensitive personal data that touches on our sense of identity has potentially far-reaching social impacts.

Challenged Identities

One can distinguish two views on identity: its socio-psychological conception, - i.e. an individual's shaping of himself, his sense of being and belonging, etc. -, and what we can refer to as its procedural one, - i.e. the formalized means of identifying an individual for the purpose of interaction and transactions with others (see Box 1).

Box 1. The socio-psychological and procedural concepts of identity

From a *socio-psychological* point of view, identity is a dynamically changing configuration reflecting, and broadly shaped by, the history of interactions between an individual and his environment, and in particular "others". Socio-psychological identity goes hand-in-hand with an individual's physical characteristics (one person/one body) and a broad range of non-physical individual and relational aspects we associate with ourselves: describing it extensively is both a private and endless task if one wants to go deeply in ones' own description[1].

Identity is characterized by aspects such as[2]:

- Permanency: It is evolving but constant in terms of time, permanent despite all change in (its) history.
- Unity: It is (perceived as) united in its diversity. Although diverse, various facets contribute to defining a single unique identity[3].
- Physical reality: It is associated with changing but again permanent "physical" characteristics, i.e. in the physical world we have one body for one identity.

From a *procedural* point of view, identity is a collection of formalized characteristics, which enable identification and authentication necessary for social and economic relations, as well as dealings with the authorities. The usual

basic ingredients are things like a person's name, marital status, date of birth, height, colour of skin or eyes, number of children, nationality, educational and professional qualifications, etc. The choice of these characteristics may depend on the context, i.e. controlling authority, functional needs, etc.

Interestingly, there is considerable interaction between both the procedural and socio-psychological facets of identity. Our procedural identity follows us formally from birth to death, it presents us as a unique individual, i.e. as citizen on an electoral role, with a unique social security or ID card number, etc. Even if it acknowledges our various roles in social life, it relies strongly on our physical presence and representation, for instance through the photos on passports and ID cards. The weakening of these interrelations underlies many of the issues raised by the future of identity in a digitized world (see Box 2).

Box 2. Historical disruptions

According to Nathalie Zemon[4] Davis, the case of Martin Guerre story[5] illustrates this concept. The story underlines the fact that when direct physical continuity is interrupted (the absence of Martin for 8 years) the relationship between the informational pattern identifying the individual and the physical entity so identified becomes problematic. Contemporary examples of historical disruptions concern cases of ID cards where the photograph of the owner could no longer be considered to be acceptably "representative", e.g. as a result of ageing.

The crucial point here is that what was an exceptional situation in the time of Martin Guerre has become the standard in the Information Society. Indeed, the Information Society, which is based on intangible assets, exchange and relation, is no longer a face-to-face culture. In this environment there is no direct physical continuity, and the historical unity of identity is lost. This therefore creates a need for a new model of identification to fill the gap of this disruptive situation.

Our hypothesis is that both facets of identity, socio-psychological and procedural, are challenged by new and future technologies in three ways:

- Identity Crisis: Socio-psychological identity results from an on-going process of "construction through interaction". Consequently, some authors claim that we are witnessing a progressive transformation of the boundary conditions of this construction process. In the emergent Information Society, new forms of communication and the emergence of new communities, sustaining in-between identities, would challenge individual and communal[6] identities. This would possibly lead to a so-called "societal identity crisis"[7].

- Digital Identities: The digitization of identity-related characteristics is progressively changing our ways of identifying individuals through their –now digital– identities: the context has changed and so with it the characteristics. Mapping digitized identities has been generating its own set of issues for the past decade.

- Virtual Identities: Networking puts the individual at the convergence point of an extended matrix of potential interactions. The dynamic process of identity-building, while taking place in a wider world of communication, and the constraints of a digitized environment offer opportunities for creating supplementary digital identities, –so-called virtual identities – for reasons of security, profit, convenience or simply fun. Virtual and multiple identities do develop and, ultimately may feed back into the "physical" world, offering a mix of physical/virtual plural identities.

Security is obviously at stake at both the individual and collective level. Identification as the entry point to defining individual responsibility, and privacy as the fundamental basis of our social structures, are both directly challenged by current and emerging trends in technology. The two following sections intend to give an insight in this evolu-

Identification as the entry point to defining individual responsibility, and privacy as the fundamental basis of our social structures, are both directly challenged by current and emerging trends in technology

tion and to identify some challenges and areas of research resulting from the growing pervasiveness of Digital Identities and from the progressive emergence of Virtual Identities.

Issues raised by the emergence of Digital Identities

Traditional procedural identity refers to a closed set of attributes defined by the context of identification. It creates a basis for identity, carefully built on long-lasting historical and political developments strongly related to definitions of privacy and citizenship. It shifts –"translates"– identity towards a narrower and restricted set of characteristics which obey the necessities of functional contexts such as the economic (i.e. commercial transactions), the judicial and social (e.g. paternity, family obligations, validation of legal documents, etc.) or the political spheres (i.e. citizenship).

Three different sets of characteristics are usually used to authenticate someone's identity: what they are (physical characteristics), what they know (personal details or passwords), or what they own (ID cards, tokens)

In turn, the digitization of identity, which is today indisputable and irreversible, comes initially from the growing amount of data accumulated by contemporary administrative practices, associated with the storage capacities and the processing power of ICTs[8].

Digital identities are either a translation of existing traditional procedural identities or a collection of fragments of either pre-existing or new data about an individual

Digital identity can be envisaged as comprising two aspects:

- a digitized version of procedural identity. It offers a "second translation" –in digitized from– of existing data collected about the individual (National ID, Social security cards, etc.)
- a pervasive means of direct association between data and individuals creating new "contextual models" of individuals through the collection, storage and analysis of digital data about them[9].

Digital Identity and authentication

As proposed by Schneier[10], one can consider that traditionally there were three sets of characteristics by which people were procedurally identifiable:

- Something one is (often in a face-to-face context): physical image, face, voice, etc.
- Something one knows and uses actively to identify oneself: name, address, social security number, etc.
- Something one owns and that represents an accepted representation of his identity: passport, token, PC card, device, etc.

Digitization of identity offers the opportunity to extend the range of characteristics in each category: biometrics, DNA, fingerprints, voiceprint, eye scans, passwords, PIN codes, smartcards, etc. The reliability of these new characteristics should be further checked in view of the proliferation of unregulated initiatives on the market.

Beyond Schneier's three categories of characteristics used for identification, networking and digitization offer the opportunity for using a fourth characteristic, namely "something one does". Indeed, our online activities are watched and captured, stored and cross-analysed by the profitable "profiling" business. Additionally, registration measures including passwords are often used to initiate and reinforce profiling by collecting data and attaching data, passwords and behaviours to a digital profile. Privacy is at stake and the process generates feed-back effects on emerging digital identities: the shapes of digital identity are built by the information system in which they take place[11].

Digital identities are either a second-hand translation of existing traditional procedural identities or a collection of elementary portions of either pre-existing or new data about an individual.

It may be that we are witnessing a splintering of procedural identity. Increasingly, identity is defined by means of a collection of digital fragments (social security numbers, electronic signatures,

and personal data). Depending on the situation (identification and authentication), systems will use only one portion of this collection although, as mentioned, identity is based on unity. Weakening the basic concept of identity raises some concern about the trustworthiness of authentication in digital environments.

Box 3. Identification and authentication

Identification is "The process that enables recognition of a user described to an automated data processing system. This is generally by "the use of unique machine-readable names"[12]. Authentication is "The act of verifying the claimed identity of an individual, station or originator"[13], in simple terms, identification asks "who are you?" and authentication asks "Are you who you say you are?"

Privacy issues

Digitization offers a unique opportunity for rapidly –albeit somewhat blindly– processing very large amounts of data. These data may be gathered over long periods of time and presented in a standardized digital format. Examples of the use of this type of data are already well known (DoubleClick, Equifax,...). Regulatory initiatives like the EU Data Protection Directive[14] are intended to ensure that proper use is made of these data.

Recent controversial uses of the archives of online forums have demonstrated the uncontrollable effects of long-term storage of individual data. Google, the biggest Internet search engine company recently bought another company, which had run a Usenet Discussion Service since 1995[15] (a database of thousands of discussion forums). After the conclusion of the financial transaction, the user's chat forum collection was copied and pasted into the database of the search engine company. Because these chat forums are still publicly accessible, a candidate for a job, say, could potentially have to deal with cynical comments he may have made years ago. Digitization offers further opportunities for such long-term storage. The "right-to-forget" is not as such part of any legislation[16], and the right to erase data about oneself is strongly weakened by the impact of database networking. This right should imply that collected personal data is erased after it has been used for the purpose for which it was stored.

Often looked upon with suspicion, anonymity is a basic feature of behaviour and a right in our societies, not for illegal purposes but in order to guarantee basic rights of privacy[17]. Storing and profiling people's behaviours on the net, or cross-checking individual data with localization technologies[18] are examples showing how anonymity is strongly endangered by the development of digital identities.

Theft of identity

Cyberspace creates opportunities for identity theft because digital records can be duplicated perfectly and leave no immediate evidence of crime[19], thus multiplying an existing risk. In 1997, A.Cavoukian[20], the Ontario privacy commissioner, defined identity theft as the acquisition of key pieces of someone's identifying information in order to impersonate them and to commit various crimes in that person's name. According to her, this area threatens to be the next growth industry in crime[21]. Recent hacking[22] and/or theft of data among major profile or credit card companies are a clear warning of the weaknesses of the system.

Some of the apparently most promising authentication techniques may have dangerous consequences. Biometrics[23] (i.e. DNA key, eye or voice-prints, etc.) is widely considered to be the most advanced and securest solution for identification or authentication because it uses characteristics that are intimately bound to a particular individual.

Digitization offers a unique opportunity for gathering and processing large quantities of personal data which may be built up over long periods of time. This raises issues of anonymity, privacy and the right to 'forget' or erase data that has accumulated on these databases

Cyberspace creates opportunities for identity theft because digital records can be duplicated perfectly and leave no immediate evidence of crime. In the case of biometrics, the harm caused by the interception of authentication information would be extremely hard to undo

Nevertheless, these characteristics cannot be replaced or modified, and if stolen there is no way of reversing the damage.

Once authentication keys are stored in digital format on network-connected databases or are transmitted over the network they are prone to hacking or interception and misuse from virtually anywhere in the world. The use of digital identities worldwide means networks have to be looked upon as critical infrastructures, both for the well being of populations and for the sustainability of the system itself. Most advanced and networked countries are also countries that face the issue of critical infrastructures in areas such as energy, transport, financial services, administration, etc.

Virtual identities, which may be created by software to offer personalized services to customers, is a type of procedural identity only loosely bound to physical reality, and which may enable users to have multiple identities

The emergence of "Virtual Identities"

Virtual identities build upon the opportunity of creating a totally virtual world of individuals (and possibly environments) in a digitized world. Virtual identities were first developed, most visibly, in on-line games such as MUD (Multi-user Dungeon or Multi-user Dimension). Since then, driven by various factors such as the explosive growth of social interaction over the network[24], the increase in people's mobility and the introduction of new means of communication, the environment has evolved and virtual identity has acquired a more serious purpose with its own potential rights and duties.

Secondly, the multiplication of registration processes on the net also encourages the trend. To avoid profiling, individuals opt for pseudonyms and develop virtual identities that are intended to have only the weakest links to real individuals. Additionally, several major companies have entered the business of on-line registration and authentication, and aim to offer users fully integrated virtual identities presented as digital passports to the cyberworld. Microsoft's HailStorm and Novell's Digitalme are examples of controversial[25] digital identity management systems. Finally, technology foresight exercises offer visions of Ubiquitous computing and Ambient Intelligence[26] worlds that refer explicitly to a further development of virtual worlds, both as multiple virtual human identities as well as virtual machine identities.

Forums, hacking activities, personal web sites that act as "virtual residences" (see Box 4) and programmable intelligent agents, –mainly search engines– are other entry points for multiplying virtual identities and pseudonyms.

Box 4. Virtual residences

The digitization of the privacy component leads to a digital version of the private sphere. With the development of new technologies related to the domestic ambient intelligence (domestic networks, gateways, home servers, etc.) the boundaries of this domestic/private sphere have evolved considerably. Observers suggest that a persona l web site with family information and services could be considered in the future as a new private sphere, i.e. a "virtual residence".

Today, virtual identities can already be borrowed or sold on the web[27]. Such identities may be valuable because they have developed their own history curriculum, for instance, in game roles or in forums and discussion groups. They have already progressed to the use of virtual payment systems such as Beenz[28] but could tomorrow be authorized to use credit cards. In this ex-nihilo world, production of multiple identities is the obvious next step, linking ubiquitously into multiple social activities.

We see virtual identity as the next step in the evolution of identity, where virtual identity:

- Is a procedural identity built mainly, if not exclusively, as a digital trace
- May be supported by some aspects of the physical world but stays largely independent of it

- May be created by software to offer personalized services to customers
- Offers the opportunity for multiple identities
- Can interact strongly with the physical world.

Identification, privacy and security of identity

Many of the issues arising out of the digitization of identities are relevant for Virtual identities. However, virtual identities extend this range of issues, offering some new potential challenges. Obviously, the identification process, whereby one specific individual is associated with a series of recognizable characteristics, is strongly challenged by the existence of virtual identities. Part of their purpose is precisely to avoid any possible correlation. Hacking activities have demonstrated this to the extreme[29]. Identification in interactions and transactions being a matter of identifying responsibility, the emergence of virtual identities and its consequences need to be better understood.

Virtual identities emerge apparently "out of nowhere" and can be pure inventions. They may also disappear equally rapidly and without trace. These are features which run counter to the "permanency" and "physical reality" criteria that are expected in any identification process correlating a physical individual to a set of digital data. Again, the longer-term consequences of this contradiction are far from explored.

Virtual identities may be considered a new way of developing privacy-related tools. Hiding behind a pseudonym that would have access to the physical world, including the ability to enter into commercial transactions, is a way of counteracting governmental monitoring or companies' profiling and surveillance. This aspect necessarily is a concern for law enforcement agencies when virtual identity feeds back into the real world.

According to the EU Data Protection Directive, information is personal if it can be associated with an identifiable individual[30]. Virtual identity does not seem to offer that protection: this new way of shaping an identity has more or less no (legal) link with an identifiable "natural"[31] individual. As a consequence, 'virtual individuals' could have no privacy rights. The concept of virtual identity could offer tomorrow a very attractive way of building up huge databases of unlimited detail within the legal framework[32].

Moreover, the ownership of virtual identities is also a thorny issue. Microsoft and Novell's initiatives on "Digital passports" have created a great deal of concern among commentators worried about the trustworthiness of such companies when compiling personal data on their customers. Associating an individual with an IP address or a number for a lifetime, in the real or the cyberworld, necessitates some precautionary thinking. Furthermore, considering that virtual identities are, to some extent, pure creations, IPR issues about one's own personal data, real or invented, could well arise. Today, some MUDs are on sale, and for quite large sums of money.

It may prove extremely difficult to establish evidence of the theft of a virtual identity. Indeed, it may be difficult to prove that it ever existed at all. As there is no correlation between an individual and a virtual identity, it will be difficult to identify the person who claims to have had it stolen from them and the damage that has been caused. Furthermore, if it does prove possible to link a virtual identity to its original owner, any damage done to others using it could be made the responsibility of that initial owner. This threat becomes a major issue for law enforcement regarding the difficulty of collecting digital evidence of cyber-crimes.

The modification of virtual identities in a database or at individual level could generate

Virtual identities emerge apparently "out of nowhere" and may last only a short time, clearly contradicting the "permanency" and "physical reality" criteria that are expected in any identification process correlating a physical individual to a set of digital data

Although virtual identities may be regarded as a way of protecting privacy, the fact that these identities are not linked with physical individuals means they lack legal protection

much more confusion than current forms of hacking. In the absence of reliable correlation between the characteristics of a virtual identity and that of a physical "model", hacking could present irreversible effects.

Conclusion

The digital world is progressively taking over some of our most important activities in relation to personal communication, commercial transactions, rights and duties. In these circumstances, security concerns and the concept of critical infrastructure rapidly come to the fore. Digital and virtual identities make us personally enter this digital world. Simultaneously, the correlation between the physical and the virtual world tends to weaken, if not disappear. Thus, permanency, unity and physical reality of identity seem less and less solid as reference points in a virtual world where tomorrow we may expect machines offering a virtual identity to chat with customers.

Identity (and its essential authenticating role in most contexts) is an evolving concept in terms of the practices developing around digital and virtual identities. The phenomenon may be seen as a major opportunity when one thinks of the numerous application domains of this evolution: customization practices, emergency services support, transport management, mobility, enhancement of human communication, worldwide access to information, services and products, reorganization of production processes, sustainability effects, etc. But one has to acknowledge the risks that exist as a consequence of the seriousness of the potential negative impacts and the growing likelihood of their occurrence.

There is obviously a need for research and proactive thinking on these aspects. As we move into the Information Society we have to acknowledge that some of the possible consequences are still unknown or poorly defined. A better understanding of digital and virtual identities, and of their possible effects, is still needed.

About the authors

Laurent Beslay has a Master's degree in International Relations (Study Institute of International Relations), for which he produced a report on "The control of exports of dual-use goods and technology, and a post-master's degree in Global Management of Risks and Crisis (University of Paris I Panthéon-Sorbonne). He is currently working on a Ph.D. on "Electronic Surveillance: benefits and risks for the European Union", while at the IPTS-European Commission, ICT unit, where he is working on the future of identity project.

Marc Bogdanowicz works as a Senior Researcher in the ICT unit of the IPTS. He has a degree in Education Sciences and Post-graduate diplomas in Organizational Sociology and in Group Dynamics Communication. Before joining the IPTS, he was in charge of the Technology Assessment Unit of the Laboratoire d'Etudes des Technologies de l'Information et de la Communication at the State University of Liège (Belgium).

Keywords

digital and virtual identity, privacy, security

Notes/References

1. In fact, one can observe that psychotherapy and personal development techniques explore these avenues.
2. Partly inspired by: "*Networked Identities, Human Identity in the Digital Domain*", Jos de Mul, ISEA'96, Rotterdam, Sept 1996.
3. This "united diversity" which generates the sense of uniqueness of identity is not equivalent to the concept of "role" which refers to our capacity to behave differently, as one same individual, in different environments such as the working environment, the family, a group of friends, etc.
4. *The Return of Martin Guerre: Imposture and Identity in a Sixteenth-Century Village*. Nathalie Zemon Davis. Cambridge, Mass.: Harvard University Press, 1983.
5. Janet Lewis's novel *The Wife of Martin Guerre* (1938).
6. Identity as a sense of belonging.
7. See i.e. Internet Society, 2001. Atelier "identité numérique", Dossier Autrans 2001. **http://www.isoc.asso.fr/autrans2001**
8. Rule J.B., "Private Lives and Public Surveillance: Social Control in the Computer Age "Rule J.B, Schocken Books, 1974.
9. *Computer Matching and Digital Identity*, 4 Feb 1993, CFP'93, Roger Clarke, Visiting Fellow, Department of Computer Science, Australian National University.

10. *Secrets & Lies, Digital Security in a Networked World,* Bruce Schneier, John Wiley & Sons, Inc, 2000,N.Y, p136.
11. According e.g. to Sherry Turkle: *Life on the Screen. Identity in the Age of the Internet,* New York: Simon &Schuster.1995.
12. Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization.
13. op. cit.
14. Directive 95/46EC of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
15. Google has acquired one of the Web's most venerated resources, Deja.com's Usenet Discussion Service in February 2001.
16. It doesn't appear clearly as a right, nevertheless the idea is already in the Convention of the Council of Europe for the Protection of individuals with regard to automatic processing of personal data ETS no.: 108, chap II, Art 5, e. and later article 6e of the EU Data Protection Directive.
17. The usual example refers to the use of cash, the most generalized and socially acceptable anonymous transactional behaviour.
18. Such as i.e. GPS and all GNSS associated projects for individual localisation.
19. The recent case of A.Abdallah, 32, convicted for invading the personal financial lives of dozens of major US corporate executives, is an example of simple and intelligent abuse of digital identities (See New York Post, March 20, 2001).
20. Identity Theft: who's using your name?, Ann Cavoukian, information & privacy commissioner/ Ontario, june 1997.
21. Indeed, according to Industry Standard Magazine, this crime was the fastest growing financial crime in the year 2000.
22. See i.e. DoubleClick under security audit after apparent hacking in march 2001.
23. "Biometrics: Uses and Abuses", B. Schneier, Inside Risks 110, Communications of the ACM, vol 42, n. 8, Aug 1999.
24. "Networked Identities, Human Identity in the Digital Domain", Jos de Mul, ISEA'96, Rotterdam, Sept. 1996.
25. One of the controversies is about the proprietary aspects of authentication in the MS initiative. But the desirability of handing over to MS databases a full range of real or virtual personal characteristics is also matter of debate.
26. See i.e. K.Ducatel, M.Bogdanowicz, F.Scapolo, J.Leijten, J.-C.Burgelman, Scenarios for Ambient Intelligence in 2010, European Commission, IST Programme, 2001. Office for Official Publications of the European Communities, Luxembourg.
27. In 2000, a couple of virtual identities built for game zone were sold on the Ebay auction website.
28. **http://www.beenz.com/index.ihtml**
29. Even if in that specific case, hackers appear to usually leave some digital trace with the aim of being ultimately recognized and acknowledged!
30. EU data protection Directive 95/46/EC of 24 October 1995, Chapter I, Art 2 definitions, (a).
31. op. cit.
32. A.Cavoukian & D.Tapscott, Who Knows : Safeguarding Your Privacy in a Networked World, Mac Graw-hill, 1996.

Contacts

Laurent Beslay, IPTS
Tel.: +34 954 488 206, fax: +34 954 488 208, e-mail: **laurent.beslay@jrc.es**
Marc Bogdanowicz, IPTS
Tel.: +34 954 488 413, fax: +34 954 488 208, e-mail: **marc.bogdanowicz@jrc.es**

ABOUT THE JRC

The Joint Research Centre (JRC), one of the Directorates General of the European Commission, carries out research and provides technical know-how in support of European Union (EU) policies. Its status as a Commission service, which guarantees independence from private or national interest, is crucial for pursuing this role.

The JRC implements its mission through specific research programmes decided by the Council upon advice from the European Parliament falling under the European Union Framework Programmes for research and technological development. The work is funded by the Budget of the European Union with additional funding from associated countries. The work of the JRC includes customer-driven scientific and technical services for specific Community policies, such as those on the environment, agriculture or nuclear safety. It is involved in competitive activities in order to validate its expertise and increase its know-how in core competencies. Its guiding line is that of "adding value" where appropriate, rather than competing directly with establishments in the Member States.

The JRC has seven institutes, located on five separate sites, in Belgium, Germany, Italy, the Netherlands and Spain. Each has its own focus of expertise.

The Institutes are:

- The Institute for Reference Materials and Measurements (IRMM)
- The Institute for Transuranium Elements (ITU)
- The Institute for Advanced Materials (IAM)
- The Institute for Protection and Security of the Citizen (IPSC)
- The Institute for Environment and Sustainability (IES)
- The Institute for Health and Consumer Protection (IHCP)
- The Institute for Prospective Technological Studies (IPTS)

Further information can be found on the JRC web site:
www.jrc.cec.eu.int

ABOUT THE IPTS

The Institute for Prospective Technological Studies (IPTS) is one of the eight institutes making up the Joint Research Centre (JRC) of the European Commission. It was established in Seville, Spain, in September 1994.

The mission of the Institute is to provide techno-economic analysis support to European decision-makers, by monitoring and analysing Science & Technology related developments, their cross-sectoral impact, their inter-relationship in the socio-economic context and future policy implications and to present this information in a timely and integrated way.

The IPTS is a unique public advisory body, independent from special national or commercial interests, closely associated with the EU policy-making process. In fact, most of the work undertaken by the IPTS is in response to direct requests from (or takes the form of long-term policy support on behalf of) the European Commission Directorate Generals, or European Parliament Committees. The IPTS also does work for Member States' governmental, academic or industrial organizations, though this represents a minor share of its total activities.

Although particular emphasis is placed on key Science and Technology fields, especially those that have a driving role and even the potential to reshape our society, important efforts are devoted to improving the understanding of the complex interactions between technology, economy and society. Indeed, the impact of technology on society and, conversely, the way technological development is driven by societal changes, are highly relevant themes within the European decision-making context.

The inter-disciplinary prospective approach adopted by the Institute is intended to provide European decision-makers with a deeper understanding of the emerging S/T issues, and it complements the activities undertaken by other Joint Research Centres institutes.

The IPTS collects information about technological developments and their application in Europe and the world, analyses this information and transmits it in an accessible form to European decision-makers. This is implemented in three sectors of activity:

- Technologies for Sustainable Development
- Life Sciences / Information and Communication Technologies
- Technology, Employment, Competitiveness and Society

In order to implement its mission, the Institute develops appropriate contacts, awareness and skills for anticipating and following the agenda of the policy decision-makers. In addition to its own resources, the IPTS makes use of external Advisory Groups and operates a Network of European Institutes working in similar areas. These networking activities enable the IPTS to draw on a large pool of available expertise, while allowing a continuous process of external peer-review of the in-house activities.

The IPTS Report is published in the first week of every month, except for the months of January and August. It is edited in English and is currently available at a price of 50 EURO per year in four languages: English, French, German and Spanish.

S.P.S.01.07

LF-AA-01-057-EN-C

The European Science and Technology Observatory Network (ESTO):
IPTS - JRC - European Commission
W.T.C., Isla de la Cartuja s/n, E-41092, Sevilla, Spain
tel.: +34-95-448 82 97; fax: +34-95-448 82 93; e-mail: ipts_secr@jrc.es

- ADIT: Agence pour la Diffusion de l'Information Tecnologique - F
- Atlantis Consulting S.A. - GR
- ARCS - Austrian Research Center Seibersdorf - AT
- CEST Programmes Ltd - Centre for Exploitation of Science and Technology - UK
- CSIC- Consejo Superior de Investigaciones Cientificas - E
- DTU - Technical University of Denmark - DK
- ENEA - Ente per le Nuove Tecnologie, l'Energia e l'Ambiente - Funzione Centrale Studi - I
- ITAS - Forschungszentrum Karlsruhe GmbH - D
- ISI - Fraunhofer Institute for Systems and Innovation Research - D
- INETI- Instituto Nacional de Engenharia e Tecnologia Industrial - P
- IPC - Irish Productivity Centre - EIR
- MERIT - University of Maastricht - NL
- OST - Observatoire des Sciences et des Techniques - F
- PREST - Victoria University of Manchester - UK
- SPRU - University of Sussex - UK
- TNO - Netherlands Organization for applied scientific research - NL
- VDI-TZ - Technology Center Future, Technologies Division - D
- VINNOVA - Swedish Agency of Innovation Systems. Innovation Policy Studies - S
- VITO - Vlaamse Instelling voor Technologisch Onderzoek - B
- VTT-GTS - Technical Research Centre of Finland - FIN

ENGLISH VERSION