European Commission
Information Society and Media

Report on the

International High Level Research Seminar on “*TRUST IN THE NET*”

Vienna, Austria, 9 February 2006

Organised by the Information Society and Media Directorate General of the European Commission, under the auspices of the Austrian Presidency

24.02.2006

This report is composed of:

- The main recommendations of the seminar (*this report*);
- The seminar agenda (*Annex I*);
- The seminar terms of reference (*Annex II*);
- The background document on “considerations and issues” (*Annex III*);
- The reflection paper “Towards increased security in electronic communications” (*Annex IV*)

I. INTRODUCTION

"We must work, pre-emptively and proactively, to build trust and security in electronic communication. What is at stake here is not just our capacity to protect existing systems, but our ability to make the Internet a key driver for European growth and societal development. Let us take the initiative now!"

(Commissioner Viviane Reding, "Trust in the Net" Seminar, Vienna 2006)

The Austrian Presidency and the European Commission's Directorate General Information Society and Media held a joint International High Level Research Seminar on "Trust in the Net" on 9 February 2006 in Vienna, Austria. The Seminar has been opened by Alfred Finz, State Secretary in the Austrian Federal Ministry of Finance and Viviane Reding, Commissioner for Information Society and Media of the European Commission. Key note addresses have been given by Rt Hon Alun Michel, UK Minister of State for Industry and the Regions, DTI and by Susanna Huovinen, Finnish Minister of Transport and Communication.

The objectives of the seminar were to discuss longer term research actions to fight malware and spam and thus improve trust in the Net for business and citizens, in particular:

- Research priorities in the seventh EU framework programme as part of the forthcoming "Strategy for a Secure Information Society" announced in the *i2010 Strategy for the Information Society;*
- Testbeds and validation actions that can advance trust in the Net;
- Types of partnership, including international ones, to be pursued and promoted in order to ensure the effectiveness of such actions as well as maximize the impact of the future research.

Commissioner Reding emphasised in her opening speech that the Seminar should also be seen as an important first step in the overall consultation process launched to identify the needs and possible actions to be taken up in her "*Strategy for increased security in electronic communications"* to be launched shortly.

On 27 October 2005 the Directorate General Information Society and Media organised a meeting with speakers in order to prepare the Seminar. This meeting resulted in a background document ("considerations and issues", *see Annex III*). This background document provided, together with the reflection paper "Towards increased security in electronic communications" (*see Annex IV*), important input to the Seminar discussions.

Discussions and presentations in the morning sessions and the two afternoon panels focused on a broad range of issues related to the notion of "trust in the net" such as risk management, identity management and privacy, interoperable authentication for electronic services, trusted computing, network security as well as technologies to support law enforcement activities. Furthermore, the participants called for coherent multi-stakeholder discussions and actions, including research, certification and standardisation, regulation and general policy strategies, aiming at a true culture of security in the Information Society.

The seminar drew some 180 participants from EU Member States and other countries, including researchers, policymakers and representatives from business and civil society communities.

II. RECOMMENDATIONS

Several recommendations with respect to *research, policy, legislation and other issues* have been put forward by the speakers, panellists and participants during the seminar discussions.

- **Research activities**

The following research issues were considered to have *high priority*:

1 The emergence of ubiquitous computing and communications calls for new solutions to deal with the *security and resilience of large, complex, open and interconnected infrastructures*, as well as for new methods for mapping and modelling the infrastructure underlying processes (e.g., *assurance* of robustness,

availability and dependability of infrastructures).

2 *Trusted computing infrastructures* built on secure platforms, networks and software ensuring interoperability and competition and enabling user transactions while respecting privacy laws.

3 A new generation of (dynamic) *reputation systems* which retain the context as well as behavioural information. Ways should be found to transfer the notion of "contact" & "reputation" from the physical world to the digital one.

4 New *cryptographic techniques* which take into account the constraints and limitations of devices and that guarantee end-to-end security in data communications.

5 Combining Network-based Intrusion Prevention Solutions (*NIPS*) and Host-based Intrusion Prevention Solutions (*HIPS*) to proactively detect intrusion both in the network and the end-devices. Methods for *network security audits, forensics and tracings*, in particular new methods for acquisition of volatile data with tools not based on the Operating System.

6 *Security of applications* and *services* and security defence measures at the "point of use" of a service, with ISP's potentially in a key role.

7 *Identification and authentication* in open, shared (federated) and dynamically changing environments. Assessing the risks when deploying *strong identification and authentication technologies* (biometrics).

8 *Privacy enhancing technologies* providing different levels of anonymity or identification and accountability for communication and on-line transactions. *Innovative Identity management systems* empowering the user, including *technologies that allow users to manage their credentials* themselves or choose to leave it to the service provider.

9 *Human Computer Interfaces* (HCI) focusing on perception and realisation by the user of security levels. Understanding the psychology of dealing with trust in the digital world without pretending to transpose the existing physical model of trust.

- **Policy and legal issues**

10 The increasing need for security will tap the potential of ICT for tracking, tracing and surveillance with unknown consequences for privacy protection and ethics. A thorough *societal debate* is needed aiming at a *balance between security, freedom and protection of human rights*, incl. privacy.

11 The role of *software* producers concerning their *responsibility* to produce, deliver and maintain secure and fault tolerant software should be further examined, i.e. software must meet a minimum set of security standards and best practice rules. A viable way to achieve this could be an industry led initiative with the support of the European Commission.

12 The *role of ISPs* with respect to the creation of trust in the Internet and the services they provide should be further examined. ISPs act as the interface of citizens and SME's to the Internet and have great potential, alone and in cooperation, to monitor, guard and improve its trust and security.

13 European policy making for Trust and Security requires a *Public-Private Partnership***,** including industry, research communities and public authorities to ensure the right balance between technology development, regulations and policy measures.

- Risk assessment, management and most importantly, allocation, are key elements of a trust framework. Support tools might be provided at the technological level, but regulatory action might be needed to allocate risks explicitly.

- Necessary R&D activities in the EU can be hindered by legislation. The increasing number of security standards and regulations in different countries should be harmonised within the EU and at a global level.
- The right balance between governance, policy and market dynamics should be investigated and the impact of security technology be looked at in terms of economics. There is a need for understanding conflicts and synergies between privacy and economics, and to produce technology and regulation that permit the desired economic growth whilst providing the desired privacy protection.

14 Security industry should change emphasis from "managing ownership for users" to "*empowering users*" to manage their own data. It should focus more on delivering security services instead of software products, providing solutions that are proportionate to the security needs.

15 It is in the security interest of the European Union to create and foster a *strong ICT security industry in Europe*, especially given that ICT is increasingly permeating all aspects of human activity.

- **Other issues**

16 A broad discussion is needed in Europe in measuring progress we make towards security in the Internet. Measurement provides us feedback on where to put our present and future efforts and could lead to a *standardisation framework* usable for the evaluation of a wide range of applications, covering both products and processes. This may require development of performance indicators, benchmarks and standardised processes to guarantee auditable levels of security in products and services.

17 Ways should be developed to effectively support *certification*, best practices and the possibility to execute risk transfer.

18 *Test beds* and large-scale demonstrators should be established *on all aspects of security and privacy*, paying special attention to information flow control and user needs. EU-funded projects, e.g. Integrated Projects could implement these test beds, to draw conclusions on the adequacy of technologies and techniques implemented.

19 *Test beds* shall also be used *to study psychological, organisational and economic aspects of trust in domains*. This could include data retention, e-government, e-health, or usage of data for customer relationship management.

ANNEX 1

INTERNATIONAL HIGH LEVEL RESEARCH SEMINAR ON

"*TRUST* IN THE NET"

9 February 2006, Museum of Modern Art
Vienna (Austria)

Organised by the Information Society and Media Directorate General of the European Commission, under the auspices of the Austrian Presidency

FINAL AGENDA

AGENDA

09:00 - 10:00 *Registration*

10:00 - 11:00 **Opening session**
Chair**: Mr. Manfred MATZKA**, Director General at the Austrian Federal Chancellery

10:00 - 10:15 Conference opening- **Mr. Alfred FINZ,** State Secretary in the Austrian Federal Ministry of Finance

10:15 – 10:30 The European Security Strategy – **Mrs Viviane REDING**, Commissioner for Information Society and Media (video)

10:30 - 10:45 Keynote address - UK Minister of State for Industry and the Regions, DTI, **Mr. Rt Hon Alun Michael, MP**

10:45 - 11:00 Keynote address – **Mrs Susanna HUOVINEN**, Finnish Minister of Transport and Communications

11:00 – 11.20 *Coffee break*

11:20 - 12:40 **The business and citizen concerns**
Chair: **Jacques BUS**, Head of Unit, Directorate General Information Society and Media (replacing **João DA SILVA**, Director, Directorate General Information Society and Media), European Commission

11:20 - 11:40 11:30 - 11:50 Keynote speaker from industry/business view
Risto SIILASMAA, CEO, F-SECURE

11:40 – 12:00 Keynote speaker from industry/user view
Sachar PAULUS, Chief Security Officer, SAP

12:00 – 12:20 Keynote speaker on citizens concerns
Malcolm CROMPTON, Former Federal Privacy Commissioner of Australia

12:20 - 12:40 Keynote speaker on public concerns
Andrea PIROTTI, Executive Director European Network and Information Security Agency (ENISA)

12:40 - 14:00: Lunch break

14:00 - 15.15 **Panel 1: Trust and certainty in electronic communications**

Chair**: Willem JONKER** (Sector Head Digital Lifestyle Technology, PHILIPS)
Stephan ENGBERG (CEO Priway)
Javier GARCIA PELLEJERO (Chief Operating Officer, ATOS Origin)
Richard COX (CIO SPAMHAUS)
Robert TEMPLE (Chief Security Architect, BT)
Michael WAIDNER (Executive Director IBM Privacy Research Institute)

15:15 - 15:45 *Coffee break*

15:45 - 17:00 **Panel 2: Identity in the Information Space**

Chair: **Geoff SMITH,** (Head, Information Security Policy, UK DTI)
Hellmut BRODA (CTO-EMEA of SUN Microsystems & Spokesperson of Liberty Alliance)
Waltraud KOTSCHY (Data Protection Commissioner, Austria)
Bart PRENEEL (Katholieke Universiteit Leuven)
Kai RANNENBERG (Goethe University)
Rolf BLOM (Ericsson Research)

17:00 - 17:45 **Moving ahead & Closure**

17:00 - 17:30 **Conclusive Remarks and recommendations**
Prof. Reinhard POSCH, Chief Information Officer for the Federal Government of Austria
Chair of Panel 1, Willem JONKER
Chair of Panel 2, Geoff SMITH

17:30 - 17:45 **Closure - The next day**
Mrs Kristiina PIETIKÄINEN (Deputy Director General of the Communications Department, Ministry of Transport and Communication Finland)

19:30 ***Reception organised by the Austrian Presidency with a speech by Commissioner Viviane REDING***

ANNEX 2

INTERNATIONAL HIGH LEVEL RESEARCH SEMINAR ON

"*TRUST* IN THE NET"

9 February 2006, Museum of Modern Art
Vienna (Austria)

Organised by the Information Society and Media Directorate General of the European Commission, under the auspices of the Austrian Presidency

TERMS OF REFERENCE

The Seminar

The Context

In its initiative "i2010 – A European Information Society for growth and employment"[1] the Commission identifies *Security* as one of the four main challenges posed by the digital convergence, which is at the heart of the creation of the single European Information Space. It states:

> ***"Trustworthy**, **secure** and **reliable ICT** are crucial for a wide take up of converging digital services. During 2006 the Commission will propose a **Strategy for a Secure Information Society** to combine and update the instruments available, including raising awareness of the need for self-protection, vigilance and monitoring of threats, rapid and effective response to attacks and system failures. Support will be given to targeted research to 'design-in' security and to deployment measures that test solutions for key issues such as identity management. Revision of regulation will be considered where necessary, for example in protection of privacy, electronic signature or discouraging illegal and harmful content."*

In addition, concerning research and innovation the Commission states:

> ***"**The co-ordination of the Commission's **research and deployment instruments** will be enhanced by focusing them on **key bottlenecks** such as interoperability, **security** and reliability, identity management, rights management and ease of use. **Research and deployment instruments will be coordinated to demonstrate technological and organisational solutions** in areas, where a shared EU level approach can help to build economies of scale and encourage investors."*

The seminar aims at discussing longer term research to create trust in the Net and fight malicious software and spam. This includes identity and privacy management, interoperable authentication for electronic services with wide recognition (reputation systems and dynamic trust marking), and technologies to support law enforcement activities.

Research & Development for Trust and Security

Significant research is already ongoing in the area of "ICT for Trust and Security" (with a total budget of 140Mio Euro for Framework Programme 6), on Identity management for eGovernment services, in eHealth related to health card and data management, and in ICT for Enterprise Networks concerning trusted business platforms and RFID.

We do now have to prepare the next Framework Programme (FP7) which, as proposed by the Commission includes such topics as:

– *Software, Grids, security and dependability*: dynamic, adaptive, dependable and trusted software and services, and new processing architectures, including their provision as a utility.

– *Personal environments*: personal communication and computing devices, accessories, wearables, implants; their interfaces and interconnections to services and resources.

– *ICT meeting societal challenges*: New systems and services in areas of public interest improving quality, efficiency, access and inclusiveness; user friendly applications, integration of new technologies and initiatives such as ambient assisted living. This is in support of health, inclusion, mobility, environment and government.

[1] COM(2005) 229 final

- *ICT for trust and confidence*: identity management; authentication and authorization; privacy enhancing technologies; rights and asset management; protection against cyber threats.

The RTD actions to be developed in FP7 must be consistent and in support of the overall strategy developed under ***i2010***. It should seamlessly connect to the deployment strategies developed in the Competitiveness and Innovation Framework Programme (CIP) and make use of research infrastructures for real live demonstrators.

Objectives of the Seminar

The seminar will bring together high-level actors from industry, research, governments, public administrations and user organisations to discuss longer term **research actions to fight malware and spam and thus improve trust in the Net for business and citizens**. The seminar should produce recommendations on:

1. Research priorities in the seventh framework programme as part of the "Strategy for a Secure Information Society announced in i2010;

2. Testbeds and validation actions that can advance trust in the Net;

3. Types of partnership, including international ones, to be pursued and promoted in order to ensure the effectiveness of such actions as well as maximize the impact of the future research.

ANNEX 3

High Level Research Seminar on *"TRUST IN THE NET"*

Considerations and issues[†]

I. INTRODUCTION

1. In the last few years the concept of the *information society* has materialized. Nowadays society makes use of, and depends on, services offered through the Internet and mobile networks, making it a chief driver for European economic growth and societal development. Taking advantage of these benefits can be impaired, however, by the perception of the public and industry that conducting business and services on the Internet may not be trustworthy enough.

2. Current threats on the Internet contribute to such erosion of trust. Well known plagues such as phishing, spam or viruses threaten the take up of ICT-based services by society and industry, and the ICT industry seems insufficiently prepared for these threats. The same plagues start appearing on mobile networks and smart phones. It is the goal of this seminar to discuss and propose the direction that European research should take in order to create the technologies that will enable the necessary level of trust in the products and processes on the Net. In addition it gives an opportunity to address other issues relevant to trust and security of the Internet and other (wireless) communication networks.

II. GENERAL CONSIDERATIONS

3. The **security of the Information Society** and its citizens is of high strategic importance for the European Union. Based on an assessment of its strengths in technology, applications and know-how decisions can be made on which technologies to invest next in this field.

4. **Industry, together with the research community leads the way in developing technologies for trust and security.** It is in the security interest of the European Union to create and foster a strong ICT security industry, especially as ICT is playing a large and still increasing role in the society.

5. The **lack of well established and unambiguous laws and regulations, and codes of conducts** on the applicability and even legality of security measures, development methods and patching of products, leaves a sort of void that businesses fill in their best interest. For instance, the important and valuable work done by anti-virus researchers in security software companies is unnecessarily hampered by existing copyright laws.

6. Given the above, there is a clear case for **Public-Private Partnerships in defining security requirements**. Industry and Research must be heard when drafting European legislation so as not to

[†] *The views expressed in this document reflect the views of the Speakers and Panellists in the discussions in preparation of the Seminar.*

prevent or hinder the necessary research and development activities in the EU.

7. **Risk assessment, management and most important of all, allocation**, is a key element of the trust framework to be further developed. Input to, and automation of, risk assessment might be provided at the technological level, but law or action by regulators might be needed to complete the process of risk allocation. In the absence of explicit allocation, risk is often carried by the weakest party, in this case the citizen or consumer. Allocation of risk towards the parties most capable of bearing and mitigating the risk has great potential to increase trust in the Net and to stimulate investments in research by those allocated the risk.

8. There is a need to investigate and understand the **psychology of dealing with trust** in the digital environment without pretending to transpose the existing physical model of trust. Trust in the digital environment is a multidimensional issue and many perspectives shall be considered.

9. The use of ICT changes the perception of security, trust and privacy. There is a need of maintaining societal and personal **"contexts" in security**. An example of creating "security in context" is moving from conventional authentication in business to novel techniques that use "profiled behaviours".

10. Security industry must be pushed to move from "**managing ownership"** for users to **"empowering users"**. This requires investment in multi-layer security focusing on empowerment with a view on self protection.

11. Security industry must move from selling licences to the delivery of security services. This is especially important to SME's, who often cannot afford their own proprietary solutions, but could choose for **remotely managed outsourced security**, charged on basis of the results obtained, if context preservation, accountability and confidentiality can be assured.

12. The approach to **security of small enterprises** is very close to that of consumers. Both need more attention and support through standardisation, certification, best practices and the possibility to execute risk transfer.

13. There are **three parallel developments**: the creation of closed user groups (e.g. based on TPM - Trusted Platform Module - technologies), secondly the increased use of technologies to spontaneously build shared networks (federations) and thirdly the use of Privacy Enhancing Technologies to maintain context in identity management. The classical approach of perimeter security is not sufficient. Strong R&D investment is needed for security and dependability of open, shared (federated) and dynamically changing environments. These technologies may enable solving seemingly controversial demands between protection of consumer rights and enforcing public safety.

14. **ISP's** play a crucial role in the creation of trust in the Internet and the services provided. They act as the interface for consumers and SME's to the Internet and have great potential, alone and in cooperation, to monitor, guard and improve its security.

15. **Wider awareness** is needed of the importance of security of information and information processing. Research on psychological issues in this context might be relevant (e.g. perception of trust, balance between security and privacy).

III. CHALLENGES AND PRIORITIES FOR FP7

III.1 Malware and Spam

16. The number one threat to the Net that can be addressed by technological enhancement is considered to be **malware** that permits unauthorised remote control of computers by "botnets". In an open networked world with the Internet at the heart, a perimeter defence is not sufficient any more and defence measures should be developed at the "point of use" of each service, with ISP's potentially in a key role.

17. We must assume that the network is insecure. Therefore, good security comprises proactive and reactive measures. The latter are well-known, reliable and necessary, even with the best proactive tools. Proactive tools may combine functionality both in the network and the end-device. Network-based Intrusion Prevention Solutions (**NIPS**) and Host-based Intrusion Prevention Solutions (**HIPS**) provide an opportunity for EU industry, as a global competitive edge can still be obtained here.

18. **Security of applications** becomes crucial within an insecure network. The weak links in this scenario are the end terminals (for instance bank ATMs, home PCs, mobile phones). In addition, gradual enhancement of technical security measures at the end points has led attackers to use different methods for remote access, e.g., the combination of technical means (man-in-the-middle) with social means (social engineering, like in phishing). The lack of authentication of banks to their on-line customers is an example of facilitating these types of attacks.

19. To support technology and legal measures against malware and spam there is a need for **network security audits, forensics and tracings**. The gradual disappearance of hard disks and their replacement by RAMs will make this task significantly more difficult, as static forensic analysis is not possible any more. New methods should be developed for volatile data acquisition with tools not based on the Operating System.

III.2 Economy and Industry

20. The **impact of security technology** should be looked at in terms of **economics**, in particular with respect to the trend for more data collection, and the need for an infrastructure enabling anonymous communication and information retrieval. Both security technology and the implementation of privacy enhancing measures require a careful approach based on European values, but without creating economic disadvantages in comparison to our competitors.

21. The Common Criteria (CC) standards are good for the **evaluation of security software for high security in very repeatable contexts, but not in the commercial one**. It is accepted that the CC are not suitable for SMEs, have limited use for standard software and cannot be applied in open environments. The lessons learnt from CC use are that we should aim at a structured analysis of security requirements and at certifying security of processes (like in the chemical industry) and not only security of products. Discussion is needed leading to a **standardization framework applicable for the evaluation of a wide range of applications, covering both products and processes for security**. The concept of "Protection Profiles" might help structuring the discussion.

22. One real challenge is to deliver **secure** and **fault tolerant software.** i.e. software that meets a minimum set of security standards (e.g. confidentiality, authenticity, integrity, access control, availability). This raises the issue of responsibility of software producers and vendors that their products are built, delivered and maintained to meet such security standards. This requires development of performance indicators and standardised processes to guarantee auditable levels of security in software. A viable way to achieve this could be an **initiative led by software industry** coupled with strategic alliances with global strong product industries, and supported by the Commission.

23. We see an increasing number of standards and regulations that affect information security in different countries. It becomes high time to **search for synergies and opportunities for harmonisation**. Currently, industry must certify their products in different countries, whilst such certifications could be arranged complementary in an integrated framework. This would benefit security and promote the advancement of the European security industry.

24. Good privacy implementation delivers accountability and security to the parties asking it. The challenge is to understand conflicts and synergies between **privacy and economics**, and to produce technologies and regulations that permit the desired economic growth whilst providing the desired privacy protection. The EU's know-how on privacy should be turned into an economic advantage.

25. We need to understand how the **Human Computer Interface** (HCI) may effectively communicate security to users and how to map preferences of users. The **perception** and **realization** by the user of security levels is an inseparable part of the set of security measures that a service must provide to an end user. There is much room for improvement and research in this area.

III.3 Trust

26. **Trusted computing** is an important technological development that should be closely followed and for which actions should be designed in order to:

    – Ensure it respects privacy laws and allows the user, rather than the manufacturer, to be in control of user data;

    – Empower the user through providing multiple choices; for instance more modes in a single machine without external control but based on distributed trust;

    – Allow for more than one security paradigm and interoperability.

27. An alternative approach is to accept an insecure network and protect data at the end points of the communication, rather than relying on the network to provide the desired confidentiality, integrity and authenticity of data. In this context the specific role of **cryptographic techniques** should be looked at by taking into account the constraints and limitations of many of the devices involved.

28. Providing "empowerment" with an angle to "self protection" needs to favour the development of a variety of interoperable security models that would **move away from monolithic trusted computing.** An important case is the handling of digital assets,

where security shall "protect" as well as "empower" the user to exploit her/his own digital assets.

29. Existing **trust frameworks are too complicated**. Target beneficiaries of such trust frameworks are "generic users" who are likely to be confused by the complications. This leads to distrust and thereby undermines the very purpose of these frameworks.

30. An important research area to be explored is that of **infrastructure assurance**. New methods of mapping and modelling the infrastructure underlying processes are needed. The ability to rely on the availability of the infrastructure when we call on it is an essential part of trust in the Net.

31. **Filtering and reputation systems** have been considered as one way to built trust, but they might not last in the long run. Therefore, further European R&D on filtering technologies is not regarded as priority. Work in this area should be left to the industry.

32. **A new generation of (dynamic) reputation systems,** which retains the context as well as behavioural information, is needed. However, the business model behind such systems might not be straightforward. The security of reputation systems in a malicious environment is inherently problematic, as attackers could manipulate the ratings of a reputation system to their benefit. Ways should be found to transfer the notion of "contact" & "reputation" from the physical world to the digital one.

III.4 Identification, Authentication and Privacy

33. Identification and authentication are essential elements for wide take-up of digital services in the Information Society. But, whilst the open character of the Internet has been crucial for its rapid economic success, it poses a challenge when it is necessary to place controls to be vigilant. The increasing need for security will tap the enormous potential of ICT for tracking, tracing and surveillance. This will raise unprecedented issues with respect to **privacy protection and ethics in the future Information Society**, which needs intensive societal debate.

34. **Privacy enhancing filtering and innovative Identity management systems are** important future R&D topics since the digital identity becomes the main "equity" in a networked society. One challenge will be the development of privacy enhancing technologies with provision of an acceptable level of anonymity in on-line transactions.

35. Many security attacks today – in particular phishing – exploit **vulnerabilities both in products and processes**. However, strong hardware-enhanced authentication processes, like for example used on GSM networks, make such attacks much more difficult. Future research might look at expanding strong authentication of users to strong authentication of networks and services. In general, we shall look at the way in which we may leverage security infrastructures that bootstrap each other.

36. The **use of strong authentication technologies** (like biometrics) should be carefully investigated before deploying them. The use of **private biometrics** with reading of data enabled in consumer devices, or behavioural authentication (i.e. context-related) should be favoured and supported.

37. Research might be needed on **devise technologies** that allow for management of user credentials by users themselves (desirable from the user's point of view), and by the service provider (desirable in cases when the user may not take proper care of their credentials).

European Commission
Information Society and Media

ANNEX 4

High Level Research Seminar on "*TRUST IN THE NET*"

"Towards increased security in electronic communications"

A Reflection Paper

I. INTRODUCTION

1. Trust and security forms an integral part of the **i2010 – A European Information Society for growth and employment**. This initiative recalls an urgent need to coordinate efforts in order to develop policies, regulations, technology and awareness to build trust and confidence of businesses and citizens in electronic communications and services and announces a new strategy to be proposed by the Commission.

2. Network and information security should be understood as one of the crucial elements of the Information Society enabling smooth development and deployment of new systems, applications and on-line services. Achieving the Lisbon strategy – that is, the goal to create a competitive, sustainable and a socially inclusive Europe – largely depends on the take-up of secure and dependable ICT across all sectors.

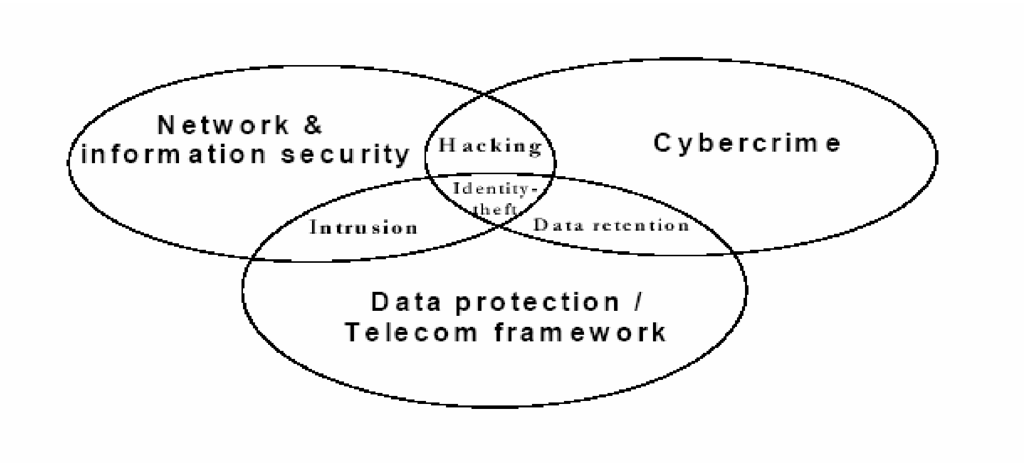
3. DG Information Society and Media has prepared this reflection paper to move forward in the discussion about how to build trust and confidence of businesses and citizens in electronic communications and services.

II. PROBLEM DEFINITION

4. Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.[3] Network and information security policy in the European Union should be seen in the context of the existing policies for electronic communications networks and services, privacy and data protection, and cybercrime, as illustrated by the following graph:[4]

[3] Communication from the Commission "Network and Information Security: Proposal for a European Policy Approach", COM(2001) 298 final

[4] *Ibidem*, p. 3


Network & information security
Hacking
Cybercrime
Identity-theft
Intrusion
Data retention
Data protection / Telecom framework

5. Network and information security is a key enabler for the further development of the Information Society in Europe and beyond. Indeed, reliable electronic communications networks and services have gained an enormous economic and societal importance as they underpin more and more many critical aspects of our economy and society.

6. At the same time, the progressing liberalisation of electronic communications networks and services markets and the resulting multiplication of actors involved, and the technological developments (to mention but two major elements) have, on the one hand, boosted competition, economic and business growth and, on the other hand, rendered the management of networks a very complex task and the division of responsibilities of various actors involved rather unclear. This is further discussed in section II.1 below.

7. A lot has been done since the adoption of the 2001 communication. However, a lot remains to be done since security problems still persist on electronic communications networks and new developments bring about new threats and disclose previously unknown vulnerabilities. Section II.2 below briefly sketches the current state of affairs.

II.1 The economic significance of information security

8. Network and information security is a far-reaching and global issue which has become increasingly important in the society based on information and knowledge. Individual users, companies and governments rely to a great extent on communication networks and information technologies. Such networks include not only the Internet, but all communications infrastructures, whether IP-based, traditional telephony or data exchange, as well as mobile networks. Their users expect reliable networks functioning without severe disruptions or interceptions and high-quality software protecting them against malicious attacks, spam, viruses and other forms of malware. Users also expect a high level of protection of confidential or personal information.

9. The economic significance of effective information security to the European economy cannot be understated. The potential economic impact of large scale failure in information systems increases in direct proportion to the ubiquity of ICTs. Accurate estimates of this potential impact at any point in time are difficult, not to say impossible, to make but some indicators highlight the scale of the economic values at risk.

10. The production of ICT goods and services in the EU for example, represent a significant part of the EU economy itself. Value added in ICT manufacturing and services represent between seven and nine percent of total manufacturing and services value added in the economy as a whole. The sector has also become increasingly important in terms of employment. In 2001 around eight percent of all employees in manufacturing and services in EU were employed in the ICT sector. The importance of the sector does not stop, of course, within the sector itself. The diffusion of ICT goods and services into other sectors also gives rise to increased productivity in the rest of the economy. Available data[5] suggests that the contributions of ICTs to GDP growth in the EU Member States ranges from 0.4 to 0.7% in the period 1995 to 2003, itself a considerable increase on the previous period.

[5] OECD “Key ICT indicators” 2005

11. Trade indicators tell a similar story. In 2004, total imports of ICT goods and services into the EU Member States amounted to more than 450 billion euro[6]. Much of this investment is going into information systems that are critically dependent on security-related performance criteria and stability requirements. Large parts of the EU economy are now either producing ICT-related goods and services or depending on them to execute their own business activities or to deliver their own ICT-based services.

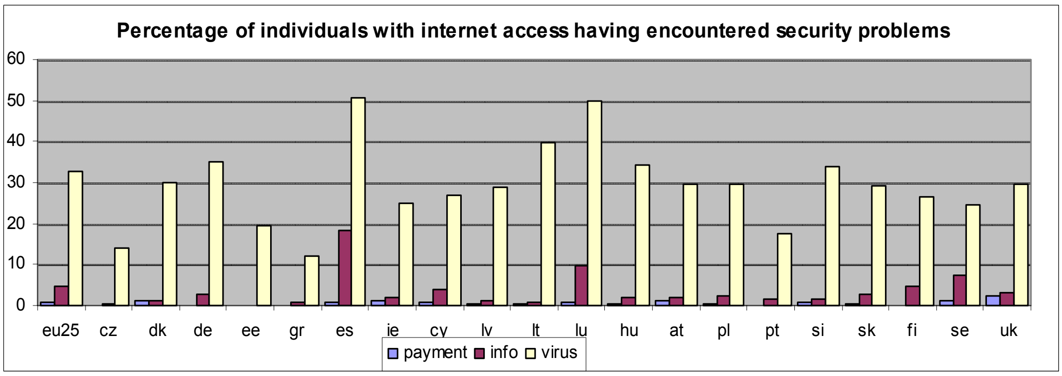
12. In the same way that ICTs can generate value-added beyond the initial economic investment, failure in ICT-based information systems can also generate a negative impact that exceeds the economic value of the systems themselves. Potential impact values will vary according to the nature and extent of the failure concerned, but will inevitably increase in general in direct proportion to the deployment and dependency of information and network systems in the economy as a whole.

13. Both the 2003 WSIS Declaration of Principles[7] as well as the recent Tunis Agenda for the Information Society confirmed that confidence and security are the main pillars of the Information Society. Therefore, there is a need to promote, develop and implement a global culture of security. From a historical point of view, concerns about information security (with a slight difference in meaning, also referred to as “cybersecurity”, “information assurance”, or “critical information infrastructure protection”) are not a new phenomenon. For instance, viruses and worms have been part of cyberspace since its early days[8]. However, the issue has gained more political impetus as communication networks and information systems have become an essential factor in **economic and societal development**. Information, predominantly in digitalised form, processed and transmitted over electronic networks, including the Internet, has become a strategically important, integral part of everyday economic and social life. Computing and networking are now becoming ubiquitous utilities in the same way as electricity or water supply already are. The security of electronic communications networks and information systems, in particular their availability, is therefore of increasing concern to EU citizens.

II.2 Current trends in information security

14. A mere look at statistics and general surveys conducted in the area of network and information security tells us that we are still far from reaching the goal of secure and reliable networks and sufficient protection of information carried on them.

15. The following data from Eurostat[9] shows the percentage of citizens and businesses with Internet connection having encountered security problems during the year 2004. The graph shows that the most important security problem which EU citizens are confronted with is the presence of viruses. More than 30 % of EU citizens reported a virus in their computer.



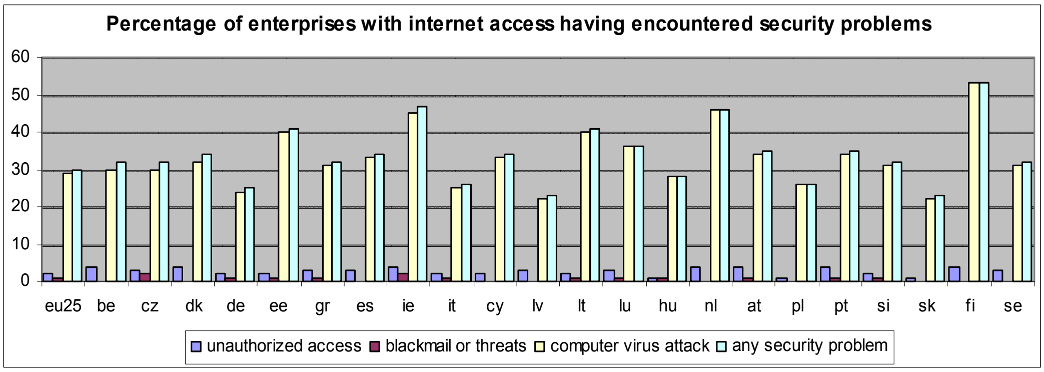
[6] OECD “Key ICT indicators” 2005

[7] Declaration of Principles “*Building the Information Society: a global challenge in the new Millennium”*, document WSIS-03/GENEVA/DOC/4-E dated 12 December 2003; and Tunis Agenda for the Information Society, document WSIS-05/Tunis/doc/6(Rev.1)-E dated 18 November 2005

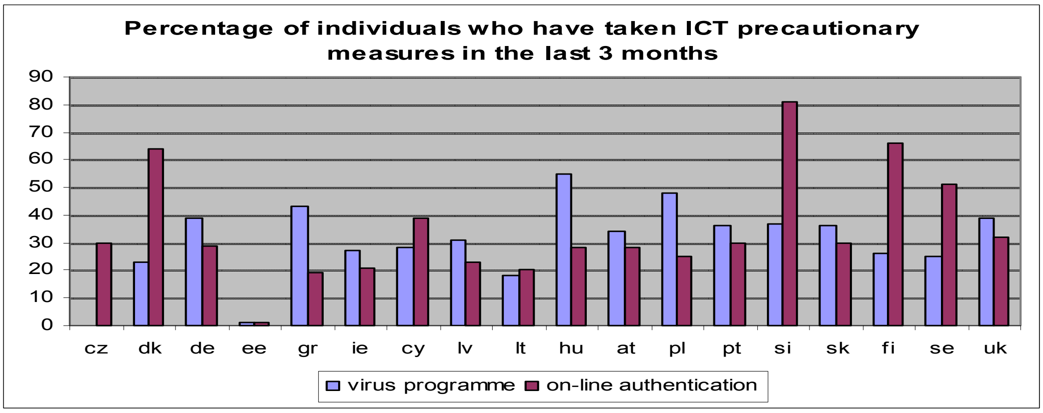
[8] E.g. the “Morris worm” of 1988

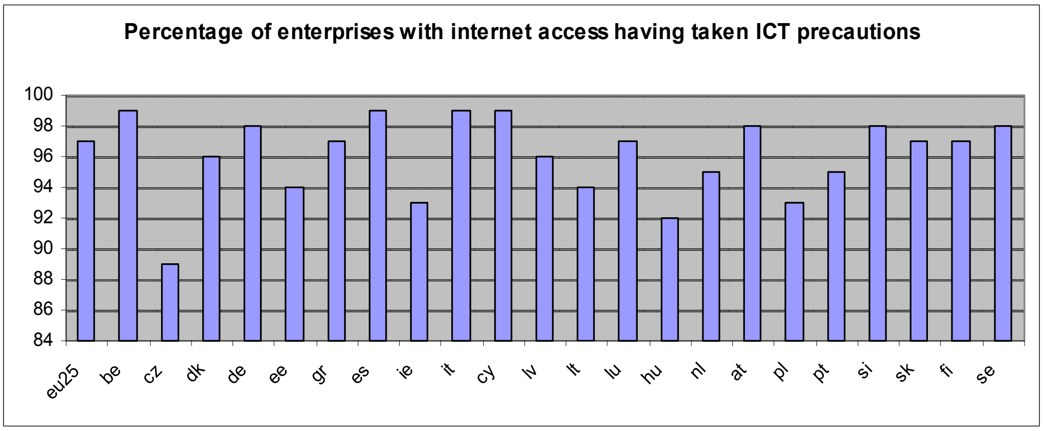
[9] The data can be accessed at: http://epp.eurostat.cec.eu.int/

16. The same situation holds for enterprises: around 30 % of EU enterprises with Internet access were attacked by a virus in 2004. 2 % of them reported unauthorized access.



17. The following two graphs show the readiness of individuals and enterprises respectively to respond to security threats. Most enterprises (97 %) in the EU 25 take precautionary measures as a reaction to security threats although the statistics does not reveal whether these measures were effective and sufficient. Percentage of individual users who have recently installed an anti-virus programme or used on-line authentication is still fairly low across the EU. The data show that there are still a relatively high number of unsafe, unprotected computers connected to the Internet.

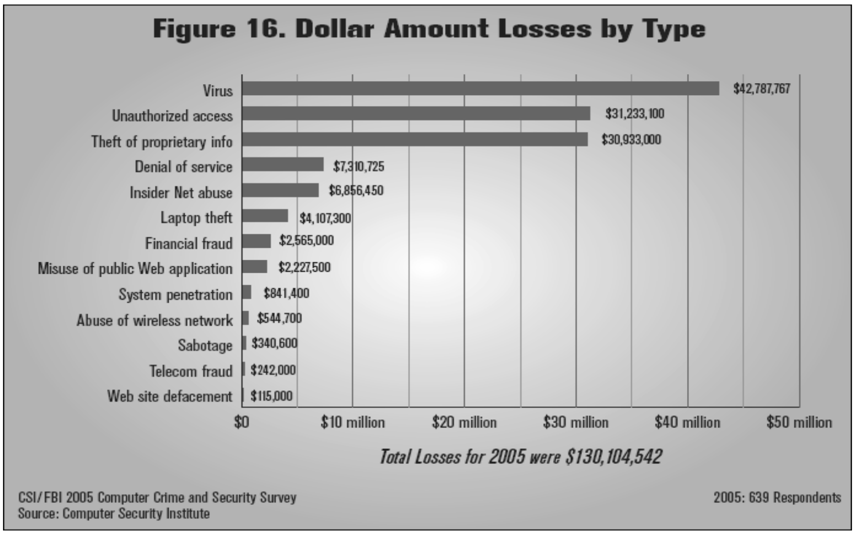




18. A couple of years ago, most security problems were reportedly caused by viruses and worms, to a lesser extent by unauthorised entry to internal networks, manipulation of software applications, identity theft or online fraud.[10] However, a recent Symantec report[11] signalled an interesting change in the "threat landscape" currently taking place. Attackers are moving away from large, multipurpose attacks on network perimeters and towards smaller, more focused attacks on client-side targets. In addition, whereas traditionally attacks have been motivated by curiosity and a desire to show off technical virtuosity, many current threats are motivated by profit. They often attempt to perpetrate criminal acts, such as identity theft, extortion and fraud. This phenomenon is sometimes summarised as a shift from a "hack for fun" to a "hack for money". Another particularly worrisome trend is the increase in malicious code that exposes confidential information, to 74 % of the top 50 malicious code samples reported to Symantec (up from 54 % during the previous reported period). This is very alarming, as threats to confidential information can result in significant financial loss, particularly if credit card information or banking details are exposed. The possibility of identity theft is of course another potential consequence.

19. The recent CSI/FBI 2005 Computer Crime and Security Survey[12] gives the following estimates of financial losses caused by various types of security incidents:

Figure 16. Dollar Amount Losses by Type



CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

20. The cost of disruption to business processes is difficult to quantify. Impact may range from nuisance (employee's productivity hindered for a few minutes) through more serious disruptions (e.g. when a corporate network is closed for repair; this is particularly harmful for organisations that rely on permanent availability of the networks 24 hours a day, 7 days a week) through loss of business opportunities.[13] One study has grouped the types of risks an enterprise faces into six major categories, with average risks per year, average IT staff hours devoted to each security incident, and average collateral damage. Keeping track of security incidents and related costs can help justify security funds and predict the probability of future incidents:[14]

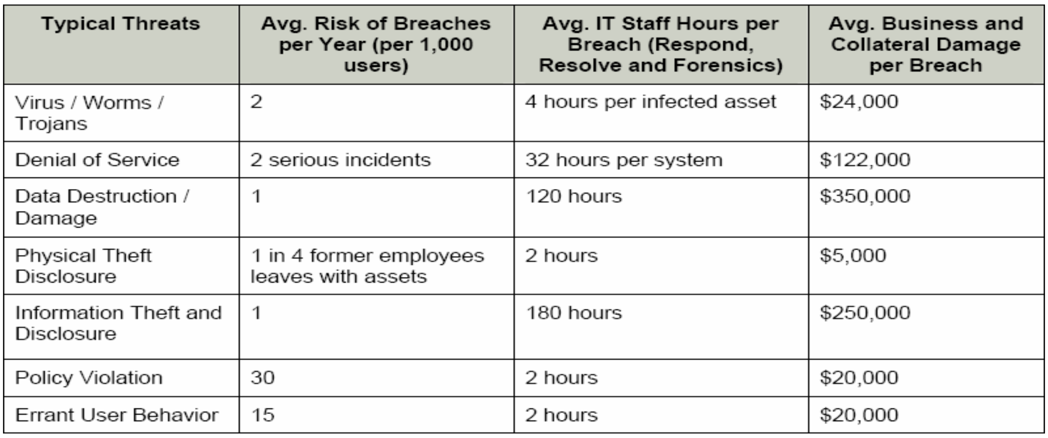
[10] The RAND 2003 survey, cited above

[11] Symantec Internet Security Threat Report, Volume VIII, trends for January 2005 – June 2005, published in September 2005

[12] 10th Annual CSI/FBI Computer Crime and Security Survey 2005

[13] "Security Breaches and the Cost of Downtime", a report by Endforce Inc., 2004

[14] *Ibidem*, quoting a report "Is There a Business Case for Security?" by Alinean, available at http://www.alinean.com/Newsletters/2004-3-March.asp



Typical Threats	Avg. Risk of Breaches per Year (per 1,000 users)	Avg. IT Staff Hours per Breach (Respond, Resolve and Forensics)	Avg. Business and Collateral Damage per Breach
Virus / Worms / Trojans	2	4 hours per infected asset	$24,000
Denial of Service	2 serious incidents	32 hours per system	$122,000
Data Destruction / Damage	1	120 hours	$350,000
Physical Theft Disclosure	1 in 4 former employees leaves with assets	2 hours	$5,000
Information Theft and Disclosure	1	180 hours	$250,000
Policy Violation	30	2 hours	$20,000
Errant User Behavior	15	2 hours	$20,000

21. According to SANS[15], a new computer connected to the Internet without firewall and virus protection will be attacked by hackers within a few minutes. Citizens who are not aware of the seriousness of various threats related to the usage of network can become not only victims of a computer attack but also a source of one. For instance, a computer - typically connected to the Internet via a broadband connection and without security software to protect it - might become infected by a Trojan horse or other malicious code and become a “zombie”, i.e. used remotely to send spam, mount denial-of-service attacks, or other online crimes.

22. Denial-of-service can be particularly nefarious for businesses relying on the Internet as they effectively aim at disconnecting networks or shutting down websites. Reportedly, this type of attack is increasingly used as an element of organised extortion schemes and has become the 4th most expensive form of computer-related crime in 2005, after virus, unauthorised access, and theft of proprietary information.[16]

23. Not only the Internet, but all electronic communications networks are vulnerable to security threats. For instance, spam, and increasingly malware, is also being distributed from one mobile phone to another (via SMS, MMS or through bluetooth connections). In addition, even if a large-scale, major global failure in a communications network has yet to happen, there have been examples of severe disruptions in several European countries in the past years.[17] This raises questions about the appropriate risk analysis and contingency planning by European operators, as well as whether adequate safeguard have been put in place by the Member States to prevent, or minimise impact of, similar failures.[18]

24. Not only are the networks vulnerable to security threats, but information technology vulnerabilities have been increasing steadily. The Symantec Internet Security Threat Report[19] monitoring computer and network vulnerabilities periodically every six months documented the highest number of new vulnerabilities in the first half of 2005 ever since the Symantec started monitoring. 97 % of these vulnerabilities were highly or moderately severe. For instance, the number of denial-of-service attacks (DoS) grew by more than 600 % compared to the previous period. Symantec reports also a strong increase in the number of variants of viruses and worms.

25. Spam, or unsolicited commercial communications, remains a serious problem. Symantec reports that in the first half of 2005, spam made up 61 % of all e-mail traffic (a slight increase from 60 % in the previous 6-month period). In addition to infringing individuals’ privacy, consuming bandwith and creating avoidable costs for consumers and

[15] SANS (“SysAdmin, Audit, Network, Security Institute”), established in the US in 1989 as a cooperative research and education organization, is one of the largest sources for information security training and certification. More information available at http://www.sans.org.

[16] 10th Annual CSI/FBI Computer Crime and Security Survey 2005

[17] E.g. the failure of the Norwegian mobile network operated by Netcom for several days in June 2005; earlier, similar problems have been reported in France

[18] It should be noted that provisions of the current regulatory framework for electronic communications concerning integrity of networks and access to emergency communications apply only to the “public telephone network at fixed locations” (Article 23 of the Universal Service Directive)

[19] Symantec Internet Security Threat Report, Volume VIII, cited above

businesses (an estimated $20 billion worldwide[20]), spam is increasingly a vehicle used for distribution of viruses, spyware and other forms of malware, as well as in phishing scams. Phishing is a form of social engineering aimed at fraudulent acquisition of sensitive information, such as passwords and credit card details. The fraudster masquerades as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message, which tricks users into giving away their account information by "confirming" it at the phisher's linked website (a link to which is typically included in the message). According to Symantec, between 1 January and 30 June 2005, the volume of phishing messages grew from an average of 2.99 million attempts a day to 5.7 million. Gartner estimates 57 million Americans have received phishing e-mails costing victims $1.2 billion in just one year.[21]

26. Another problem increasingly associated with computer security breaches is identity theft (ID theft), i.e. the deliberate appropriation of another person's identity, usually to gain access to their finances (and for instance obtain loans and buy goods in the victim's name). Less commonly, it's purpose is to enable illegal immigration, terrorism, espionage, and the like.[22] Techniques for obtaining identification information range from the crude, such as stealing mail or rummaging through rubbish ("dumpster diving" in the US), stealing personal information from computer systems and networks, to infiltration of organizations that store large amounts of personal information.

27. Until recently, the term "identity theft" seems to have been more widely used in the United States than in Europe.[23] One reason could be that ID theft is usually the result of serious breaches of privacy whereas processing of personal data and protection of privacy is covered appropriately by European legislation. Another reason could be the widespread use of publicly available data (e.g. social security number or driver licence details) for identification in the United States.[24] However, many governments like the United Kingdom now claim that ID theft is the fastest growing offence when using electronic communication services. It is estimated that more than 100,000 people are affected by identity theft in the UK each year, costing the British economy over £1.3 billion annually.[25] ID theft is also gaining an additional dimension in the light of the fight against illegal immigration, terrorism, and organised crime.

28. It is important to note that identity theft and related crime are not exclusively, or even predominantly, related to the use of the Internet or involve the use of computers. The US Federal Trade Commission reported in 2002 that only 13 % of victims of ID theft identified "transactions" as the mechanisms leading to the crime – and this covers both on-line and off-line transactions. On the other hand, it seems safe to assume that at least part of the cases is linked to attacks on computer systems and networks.

29. It is difficult to fully quantify the extent of real ID theft and consequently it is difficult to compile sound statistics. On the one hand, ID theft is often followed by other crimes such as fraud; on the other hand, it is hard to detect because personal data is not stolen physically but is "just" copied. Nevertheless, with the growing deployment of e-commerce, e-business and e-government services more and more personal data is transferred via electronic communications networks. This in itself could increase the risk of ID theft if the data is not sufficiently secured. In

[20] Business Software Alliance, September 2005

[21] *Idem*

[22] http://en.wikipedia.org/wiki/Identity_theft. On the other hand, Assuming a false identity with the knowledge and approval of the person being impersonated, such as for cheating on an exam, is not considered to be identity theft. The UK Home Office Identity Theft Steering Committee proposes the following definitions: *Identity Crime* as a generic term for Identity Theft, creating a False Identity or committing Identity Fraud (a *False Identity* being either fictitious (i.e. invented) or a genuine identity that has been altered to create a fictitious identity); *Identity Theft* occurs when sufficient information about an identity is obtained to facilitate Identity Fraud, irrespective of whether, in the case of an individual, the victim is alive or dead; *Identity Fraud* occurs when a False Identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Fraud.

[23] A 2003 survey by the US Federal Trade Commission showed that over a one-year period nearly 10 million people – or 4.6 % of the adult population of the country – had discovered that they were victims of some form of identity theft. See "Identity Theft Survey Report", September 2003, available at: http://www.ftc.gov/os/2003/09/synovatereport.pdf. Similar statistics for Europe are not available.

[24] In the US, knowing the SSN of a person is often treated as sufficient identification that you are that person. The widespread use of both official and private databases which hold SSN opens the door to large-scale identity theft. In addition, geography and commercial habits in the United States have led to long-distance transactions being much commoner than in most of Europe, which may at least partially explain the spread of identity theft in the US. See "*Identity Theft. A Discussion Paper*", European Commission, JRC, 2004

[25] Source: Home Office Identity Theft Steering Committee, http://www.identity-theft.org.uk/

addition to eavesdropping during transmission or unauthorised access to information systems storing the data, phishing also carries threat of ID theft. Carefully designed and correctly implemented identity management solutions could provide a remedy. Of course, EU legislation in the field of data protection and cybercrime is likely to contribute to reducing the risk of ID theft. In particular, the recently adopted Framework Decision on Attacks against Information Systems requires Member States to criminalise illegal access to information systems which often constitutes an important element of ID theft-related crimes. In addition, Article 4(2) of the ePrivacy Directive (2002/58/EC) provides that the electronic communications service provider must inform the subscriber of a particular risk of a breach of the security of the network.

30. The scope of security threats is already very wide and is expected to widen even further with new technologies arriving on the market, such as wireless technologies, voice-over-IP (VoIP), etc. Some industry analysts believe that 50 % of the world's telephone traffic may be based on VoIP by 2006.[26] In addition, there are indications that security problems associated with mobile computing (the use of laptops, PDAs, smartphones, etc.) might become the most important information security issues over the next few years. A recent study points out that one-third of professionals who use mobile devices do not protect the data they contain with passwords or any other type of security measure. 30 % use the devices to store PINs, passwords and other sensitive corporate data, including customer contacts. 22 % of those surveyed said they had lost a mobile device; of those, 81 percent had not encrypted the data on the device.[27] Clearly, not all organisations have sufficiently addressed these issues in their security policies.

31. According to the OECD[28], a number of factors are likely to contribute to continuing vulnerability in the coming years. These include:

- The introduction of entirely new and potentially more destructive forms of malicious code and cyber attacks;
- The proliferation of new web applications, often with easy-to-exploit remote accessibility;
- The spread of instant messaging and peer-to-peer applications;
- The growth of mobile devices with always-on connectivity and remote access to critical sensitive data.

The study concludes that "as the vulnerability of information systems persists and evolves, demand for information security – both for physical security and access control (e.g. biometrics, encryption login) and for operational security (firewalls, anti-virus software etc.) – is expected to grow."[29]

32. During the recent ISSE 2005 conference in Budapest, ENISA polled the audience about the state of Internet security, future threats and best ways to address them at European level. According to the delegates, the major threats to the Internet in the next five years will be mobile security threats (38 %), ID theft and *phishing* scams (21 %). DoS attacks scored 12 %. Only 2 %, believed hacking would be the main problem in the future. As for the most effective European approach to deal with Internet security threats, the audience supported "creating user awareness" as the most effective method (47 %). 23 % thought facilitation of industry co-operation would be most useful, whereas 17 % think enforcement and 13 % regulation are the ways forward. No support was voiced for a "do nothing" option. In addition, the poll demonstrated quite a high level of support for involvement of European institutions and bodies in addressing security threats on the Internet (average score of 7.34 out of 10).

33. All in all, information security is a broad and complex field where no easy and ready-made solutions are available. Therefore, decision-makers and regulators must try to find the right mix of regulation, competition and co-ordination creating the right incentives for the private sector in order to ensure a minimum level of security, proper risk assessment, prevention and general public awareness.

[26] OECD Communications Outlook, 2005

[27] Pointsec's Mobile Usage Survey, 2005

[28] "The Security Economy", OECD, 2004

[29] *Idem*, p. 30

III. Conclusions

34. DG Information Society and Media hopes that this reflection paper will stimulate a debate about the future policy options on network and information security. We look forward to receiving feedback from all stakeholders.