SecurIST Advisory Board

Recommendations for a Security and Dependability Research Framework:

from Security and Dependability by Central Command and Control to Security and Dependability by Empowerment

Issue 3.0
15 January 2007

Project no. 004547

Project acronym: SecurIST

Project title: Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D *(Steering Committee for a European Security & Dependability Taskforce)*

Instrument: Coordinating Action

Priority: SIXTH FRAMEWORK PROGRAMME

PRIORITY 2

Information Society Technologies

SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework

From "Security and Dependability by Central Command and Control"

to "Security and Dependability by Empowerment"

Issue 3.0

15 January, 2007

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
Public	Public for interested parties involved in preparation of Work Programme for FP7.	

Part I - SecurIST Advisory Board Recommendations

Table of Contents

Management Summary 5
1 Introduction 7
1.1 The SecurIST Advisory Board 7
1.2 Security and Dependability in the first Decade of the 21st Century 7
1.3 Globalisation 8
1.4 European Activities 9
2 The Information Society Stakeholders 10
2.1 The Stakeholders 10
2.2 The Citizen's Perspectives on Security and Dependability 11
2.3 Organizations' Perspectives on Security and Dependability 13
2.4 Core Concepts and Their Issues 14
2.4.1 Digital Identities 14
2.4.2 Channel Management 15
2.4.3 Information Privacy 16
2.4.4 The Applications and Services considerations 16
2.4.5 Infrastructure Dependability 18
2.4.6 Technologies for security provision 18
3 Research areas to be addressed 21
3.1 Empowerment of Stakeholders 21
3.2 Europe-specific Security and Dependability 23
3.3 Infrastructure Robustness and Availability 23
3.4 Interoperability 24
3.5 Processes for developing more secure and dependable systems 24
3.6 Security and Dependability Preservation 25
3.7 User centric Standardization 26
3.8 Security and Dependability of Service-Oriented Architecture 26
3.9 Technologies for security 28
4 Preview – a longer term vision of research in security and dependability 30
4.1 Overview 30
4.2 Security and Dependability – four Grand Challenges 31
References 33
Glossary 35
Annex I – Advisory Board Members List 47
Annex II – STF Challenges Aggregated to Seven Key Focus areas 49

Management Summary

The SecurIST Advisory Board has undertaken the task of examining the requirements for the European Security and Dependability Research Framework from the perspectives of the Information Society's various stakeholders, with a particular focus on those of the individual or citizen within this Society. The information systems that make up the European Information Society in this context consists of hardware, software, processes and people, thus covering non-technical as well as technical aspects. Stakeholders of the Information Society include (but are not limited to) individual citizens, SMEs, large corporations, non-governmental organisations and governments, and indeed the research community itself.

The Advisory Board believe that it is important to address all the different facets of security and dependability in the European Information Society. Dependability is an integrating concept that encompasses the qualities or attributes such as availability, reliability, safety, integrity, and maintainability, and mainly seeks to achieve these attributes in the face of possible accidental physical and design faults. Security is seen as encompassing the confidentiality[1], integrity and availability of information and seeks to preserve these properties in the face of any threat that may compromise them such as software failure, human error or deliberate attack. The two concepts, overlap extensively, and are closely inter-related. In order to get the maximum benefits of research results going forward, an interdisciplinary and integrated approach is required which goes beyond focussing on narrow technological issues.

The SecurIST approach is complementary to the approach by the European Security Research Advisory Board ESRAB [1], which is rather focused on security from a government and enterprise perspective and to the work of the European Network and Information Security Agency ENISA [2], focussing on best practices in Computer Emergency Response Team (CERT) co-operation, risk management and awareness.

There are many stakeholders in the European Information Society and it is important to look at problems, needs and solutions from the perspective of them all. However, the problems and needs of individuals deserve a particular focus. End-users, in particular individual citizens are, understandably, becoming more and more concerned about the increasing complexity of information systems, about the trend toward central control and monitoring in electronic environments and about the continued attempts to make every digitized action accountable by associating it with identities that lead back to individual citizens, corporate entities or members of organisations. To keep up to date with the increasing rate of change of the information society, the end-users find themselves having to put ever more trust into environments they have no way of understanding or assessing. In other words, the risk of using the Information Society's processes and systems appears to be increasing: risks such as identity theft and abuse; disclosure of sensitive information; wrong attribution of charges – *financial* or *criminal*. Currently, such issues are evolving trends only, so for a secure and dependable Europe there are challenges but there are also opportunities. Focused correctly, research for a secure and dependable Information Society can lead the way towards a future environment in which the risks to the various end-users, in particular to individual citizens, of living in the Information Society are significantly lower than they are today.

The Advisory Board has come to the conclusion that given these trends, if there is to be a secure and dependable future Information Society in Europe, the following nine key areas need to be addressed in a European Security and Dependability Research Framework: These are outlined on the following page. In addition to these nine key areas, four future *grand challenges* are given that illustrate possible longer-term possibilities and implications. While offering new freedoms and opportunities, they also present new and dangerous security and dependability risks to the individual and to society, and set new challenges to the research community.

The Board's report, recommendations and review of requirements, is contained in Part 1 of the document; Part 2 contains an extensive glossary and informative annexes.

[1] including privacy aspects

Key areas for a European Security and Dependability Research Framework

1. Empowerment of the various types of Stakeholder, and in particular of Citizens:
Empowerment of the citizen [3] is vital as there is a clear technological trend towards the decentralization of technology and its management and control. Current centralized control structures need to be enhanced or perhaps even replaced, since security and risk management considerations, e.g. concerning identity theft, in fact imply that responsibility, authority and control have to move more towards the end user. If the user is to be accountable, then the user must have proper protection and control.

2. Europe-specific Security and Dependability:
Europe has a very particular yet heterogeneous culture, history, and set of attitudes to trust and society. The European Information Society will have the possibility to compete successfully with information societies being established in other regions of the globe if and only if Europe-specific needs are taken into account and actively addressed by technological and socio-technical research projects in a structured manner.

3. Infrastructure Robustness and Availability:
As stakeholders come increasingly to rely on ICT infrastructure, covering both local infrastructure such as software, and hardware devices, and network infrastructure, involving various communications technologies, the assurance of the robustness and availability of the infrastructure grows in importance. Over and beyond ICT infrastructure, there is an evident requirement for reliable and available critical infrastructures such as medical, energy, telecommunications, transport, finance, administration and emergency services.

4. Interoperability:
The future is unlikely to be a homogeneous, standardized technology for communications purposes, but rather a whole range of fixed and mobile communications technologies, ranging from body area networks to broadband broadcast communications across national borders. If this complex web of technologies is to function effectively, it is crucial that there will be semantic interoperability between security and dependability technologies.

5. Processes for developing more secure and dependable systems:
There needs to be systematic improvement of methods of developing secure and dependable systems, including hardware and software, right from the beginning of the development process, whether one is constructing an entirely new system, or one composed of pre-existing systems.

6. Security and Dependability Preservation:
Once systems have been developed and installed, the maintenance of effective system security and dependability is critical. This is particularly true in an increasingly complex world of evolving requirements, technologies and systems. Preserving security and dependability also means preserving the confidence users have with regard to information privacy, transaction correctness, etc.

7. User-centric security and dependability standardization:
Strengthening of the structured involvement of end-users, in particular citizens and their respective representatives or institutions, into all relevant security and dependability standardization activities.

8. Security and Dependability of Service Oriented Architectures (SOAs):
Means are needed to establish and maintain trust and to manage policy regulations and Service Level Agreements regarding security and dependability, in an SOA context, together with commensurate advances in software engineering to deliver service expectations.

9. Technologies for security:
Underlying all of these is the need to provide higher assurance of trusted communication and handling of digital information. The two fundamental sciences and technologies are (a) cryptology and (b) trusted functionality and computing. Cryptology ensures the protection of information stored or in transit outside a trusted area. The trusted functionality creates and maintains that trusted area, and ensures that information is handled within it as intended, and that the cryptographic processes are correctly executed. Security protocols establish and maintain trusted communication between trusted areas. Both disciplines need sustained R&D to keep ahead of the needs of their dependants.

1 Introduction

This Report is structured into four chapters. Chapter one represents the rationale and introduction, highlighting the security and dependability situation in the first decade of the 21st century. Chapter two discusses security and dependability requirements of the European Information Society's citizens and what is involved in providing these requirements. Chapter three explains the key recommendations in detail. A fourth chapter presents possible future challenges that illustrate the need to be already prepared for new scientific and technological developments and directions. A list of references, an extensive glossary, and informative annexes complete the Report.

1.1 The SecurIST Advisory Board

The SecurIST Advisory Board [Annex I] is composed of European experts in Information Security and Dependability and has the task of reviewing results from the Security and Dependability Task Force. The Advisory Board has met physically a number of times, and were presented with the challenges identified by the different Task Force Initiatives and the rationale behind the challenges. The Advisory Board has prepared documentation and given presentations on its preliminary findings [4]. The Board also has established and will continue establishing links to other relevant European activities and bodies that are of relevance to security in the future European Information Society, such as the European Security Research Advisory Board ESRAB, and the European Network and Information Security Agency ENISA.
The SecurIST Advisory Board members' personal reputation and competence, their extensive experience and their well-established contact networks in Information Security have been used to build and promote a consolidated picture particularly, but not solely from a citizen's perspective, of the future Information Society. This is the subject of the present report.

1.2 Security and Dependability in the first Decade of the 21st Century

Security and dependability have been continuously among the key issues on the list of the European Council's presidencies and will remain a major challenge to Europe and to the global community for the upcoming years. Terrorist attacks have become a global threat and society becomes more and more dependent on critical infrastructures of ever greater (indeed in many cases unmastered) complexity. Therefore, security and dependability research must be focused on the right topics and a research agenda must take into account different facets of the broad subject area of "security and dependability". These facets include physical security, electronic security, critical infrastructure protection and IT security, in the face of deliberate attacks, and both system and infrastructure dependability and indeed security, in the face of physical malfunctions and residual design defects.

Dependability is an integrating concept that encompasses the following attributes: availability, reliability, safety, integrity, and maintainability, and mainly seeks to achieve these attributes in the face of possible accidental physical and design faults. Security is a concept encompassing the confidentiality, integrity and availability of information and seeks to preserve these properties in the face of any threat that may compromise them such as software failure, human error or deliberate attack. The two concepts thus overlap somewhat, and are closely inter-related. Successful security breaches commonly are based on exploiting vulnerabilities that exist as a result of residual system design faults or during periods of physical failures, and dependability can be badly affected as a result of unauthorised actions that were not prevented by appropriate security mechanisms. In what follows, therefore, the phrase "security and dependability" occurs frequently – a possible abbreviation for this phrase is "trustworthiness" [5]. However, effective security and dependability research will need to broaden its scope from purely technological aspects and to address related areas with equal emphasis, e.g.:

- Interdisciplinary approaches
- Socio-technical research,
- Industry trends (e.g. such as outsourcing and offshoring)
- Co-ordination between policy makers and technical research.

The evolution of our digital society is characterized by ubiquitous computations, communications and storage, and by the development of services that are personalized and context-aware. In the coming

years, we will notably see the deployment or emergence of new information and communication infrastructures like converged mobile and fixed networks based on the IMS architecture, WiMAX networks, corporate networks with Voice over IP or multimedia, Peer to Peer structures, networks of sensors/actuators with scarce data-processing resources or the *Internet of Things* [6].

The trend is towards the emergence and deployment of ever more massively distributed, interoperable and interdependent complex ICT systems composed of billions of interacting components whether fixed or mobile. Their emergence will create new, unprecedented challenges for Security, Dependability and Trust as for example: security and dependability of Beyond-3G infrastructures and the new cellular networks (security of mobility, services and their supervision); trust, security and dependability of post-IP networks, in particular the Future Internet, also in relation to international work in this area (NSF initiatives FIND, GENI) and trust, security and dependability attributes in the architecture and design of future networked systems, as for example new protocols, adaptive detection, diagnosis, and run-time response mechanisms and stochastic security in core/access networks from an end-to-end perspective; the protection of critical infrastructures and their interdependencies; security and dependability of software systems and services including security and dependability of overlay networks, overlay services (dynamic virtual systems), security of the virtualisation paradigm (horizontal and vertical hand-overs and associated security, nomadic fast authentications, services in real time, massively distributed, multi-users, management of these services.

At the smallest level, nanotechnology, quantum communication and cryptography offer new opportunities to tackle ICT security. Embedded sensors and devices can form ad-hoc networks requiring new mechanisms for establishing trust when sharing information or resources. New paradigms come to the foreground, such as service architectures that compose services from lower level modules, peer-to-peer systems characterized by their remarkable robustness and resilience against attack, and biological defence mechanisms, which may inspire new breakthrough technologies. At a larger scale, the completion of the Galileo satellite navigation system around 2009 will create ever more sophisticated possibilities for positioning with implications for both security and privacy.

Against this background, this document presents the view of the SecurIST Advisory Board on the security and dependability challenges and requirements for the Information Society in Europe. It is based on the work of the board members during 2005 and 2006, as well as on several meetings/workshops and it takes into account the findings and challenges listed in the report from the Security and Dependability Task Force [7]. The document is meant to complement the preliminary findings of the European Security Research Advisory Board ESRAB and work of the European Network and Information Security Agency ENISA, by adding the European Information Society citizens' perspective on security and dependability.

1.3 Globalisation

Globalisation is already having a major impact on all the countries in Europe, and the role of the European Union is therefore two-fold, aiming at internal and external goals: the future European Information Society will have to create interconnectivity and harmonisation between the European Member States and will also have to find its role in the global environment with American and Asian markets that are competitors and partners at the same time.

Information is already considered a valuable commodity, but present and future information networks do not end at national borders nor is there any strong separation between the United States, Europe and Asia. Physical infrastructures are merging and converging; virtual networks, ubiquitous computing and ambient networks have started to replace today's concepts of central network control. The same interdependency that is visible in communications infrastructures is partly also occurring for other critical infrastructure sectors such as power and energy supply, transport and financial services. The effects of faults, whether accidental or deliberate in origin, can if not adequately controlled, cascade from one system to another, and have catastrophic effects on the reliability, availability and security of these systems. The challenge for the future European Information Society, therefore, is neither limited to the geographical area of Member States nor can it be addressed by European regulations alone. A balance must be maintained between playing a fully participating role in the global enterprise and the need to avoid domination and control of our essential infrastructures by non-European interests.

Furthermore, the competitive situation, especially towards a highly advanced IT and security technology market in Northern America and a low-cost high-speed development in South-East Asia, forces Europe to find its own position with respect to security and dependability in general and IT security and dependability specifically. The very strengths developed by Europe in the area of security and dependability provides a significant opportunity for their exploitation, and the provision of solutions worldwide.

1.4 European Activities

In a European environment, security and dependability are discussed in various contexts, including areas such as

- The role of Europe in the world-wide fight against terrorism,
- European border control across now 27 member states,
- IT security activities as addressed e.g. by the European Network and Information Security Agency ENISA,
- A dedicated European Security Research Programme ESRP as part of the 7th Framework Programme,
- Protection of the future European Information Society with special attention to the Information Society citizens' requirements,
- The robustness of the Information Society's systems and infrastructures on which citizens are expected to place ever greater dependence and trust.

2 The Information Society Stakeholders

2.1 The Stakeholders

The European Information Society has a range of stakeholders, including SMEs, large corporations, government departments, non-governmental organisations and individuals in the role of employee, consumer, shareholder and citizen. Each category of stakeholder has a number of problems and issues facing them regarding security and dependability.

The information and communication systems of large corporations are often complex systems working across many countries and used by thousands of employees. Many external parties, such as, suppliers and customers, also access these systems. In attempting to achieve systems that are secure and dependable, large corporations have to balance the risks they face from threats to their systems against the cost of security and dependability measures. Although they have specialist staff to design and develop their systems and to advise on security and dependability issues, they often face problems. What are the risks? Is there good data on threats and their likelihood? What is best practice in dealing with this new technology? What vulnerabilities will this new piece of technology introduce? What legislation and regulations affect this system? What controls will regulators demand? How much should be spent on protective measures? And these problems often have to be addressed in a difficult and competitive economic environment.

National and European governmental organisations share many of the problems of large corporations in terms of security and dependability. They often have large, complex systems, huge databases and thousands of people needing access. In building and operating their systems, government departments face the same problems regarding risks, availability of sound data, best practice and so on.

SMEs have the problem that they are too small to have several different experts on their staff to address the full range of security and dependability issues. Ideally, they would like to buy secure and dependable components that they can join together into a secure and dependable system. In essence, they need 'plug and play' security and dependability. Today, this is not really available.

Individuals also face problems regarding security and dependability, which vary depending on their particular role, such as employee or citizen. Although individuals understand security and dependability regarding physical items, such as their house, they do not have a clear understanding when it comes to their digital presence. Information and Communication systems are becoming increasingly complex and individuals are having to trust systems they do not really understand and are not fully aware of the risks involved.

The university and research institution networks have many of the characteristics of the large commercial and administrative organisations. They have an important role as both researchers and educators, but they also must also ensure that malware – perhaps generated by students out of a misplaced sense of playfulness or power – is captured, and not allowed propagate.

The problems that all stakeholders face will increase markedly as the development of the European Information Society gathers pace. In the digital world of tomorrow:

- The number of devices connected to the Internet will grow by an order of magnitude,
- New technology, such as GRID and RFID will become commonplace,
- Computer and Communications technology will have converged and will be considered as a utility like electricity,
- Access to the Computer and Communications utility will be from anywhere at any time, with seamless hand-over from fixed to wireless, and from personal networks – body, home, car – to local networks to mobile networks to an employers network.

In this environment, it is clear that the security and dependability challenges will become significantly greater and any research agenda must address the problems and issues faced by all stakeholders in the European Information Society.

However, if the above developments are inspected more closely, a number of trends can be identified:

- There is a decentralisation of technology, which implies a decentralisation of control. Many devices will communicate with other devices and this has to be under direct or indirect owner control.
- In a digital world, the importance of identity becomes critical and the management of identity by the various types of stakeholder, and in particular by individual citizens, takes on added importance.
- As the digital world begins to affect almost all facets of an individual's life, there will be greater concern about security, dependability and privacy.
- Since data is a critical resource of the information society, ensuring the control of data is in the hands of end-customers is critical to ensure that applications and services offered by value chains will align according to human needs.

The Advisory Board, therefore, believe that the needs and concerns of the individual citizen will have a profound effect on the development of the European Information Society and that particular attention should be paid to these needs.

However, it must be stressed that the solutions that emerge from research into the citizen's needs will also have a beneficial impact on the needs of all the other types of stakeholder. All large information systems involve both ICT and people. Even with dependable ICT, people are still a weak point and a prime source of security and dependability problems, e.g. through uninformed actions, or through deliberate misconduct. Thus strengthening client-side security and dependability is vital for progress:

- All value chains end in personal consumption – by focussing on client-side security and dependability, we ensure that value chains align according to customer needs and preferences as the main driver for growth. For example, organisational or server-side database security depends on user security. If you can successfully steal the identity of a security-cleared operator, you can always break into an ICT system.
- Perimeter security is failing- we have to move to security paradigms based on Security by Design.
- Citizen security is a precondition for democracy.
- We need balanced security and dependability – otherwise one citizen's protection turns into a threat to other citizens.

As the digital world begins to affect almost all facets of each individual's life, there will be greater concern about security, dependability and privacy. What is key to the position of the Advisory Board is that all security and dependability is integrated – to secure ICT we both should and need to include Citizen self-protection, as ICT security and dependability cannot be better than Citizen security and dependability. We need alignment and holistic approaches to security, dependability and privacy.

2.2 The Citizen's Perspectives on Security and Dependability

The SecurIST Advisory Board has aimed to provide a particular perspective on security and dependability from the standpoint of the citizen of the Information Society. The citizens' perspectives are, in the Board's view, characterized by the following attitudes that are unique to citizens:

Citizens will not use systems and services unless they are forced to, or can see that it is in their best interest to do so - this latter will not be the case unless they have reason to believe that the systems and services are performing correctly and efficiently, and are useful, usable and understandable. Purely technical solutions that do not take into account personal preferences, and human capacities and frailties are unlikely to be sufficient.

> *Citizens place a high valuation on their individual personal data:*
> In a company and government environment, protection of employee and company/government data is mostly enforced by policies and organization specific rules. In contrast, the genuine citizens' perspective does not consider company data or third party data but is focused on the protection and privacy of personal data and identities related to the individual citizens as end-users.
>
> *Citizens increasingly distrust ICT services and infrastructure:*

The citizen's experience in many cases is dominated by publicity about computer failures, huge unsuccessful system development projects, malware (e.g., viruses) and spam mail. In contrast to sharply focused company environments that are only accessible to an exactly specified set of employees, one has to assume that, due to the negative publicity, the average citizen will place only very limited trust into public ICT services, systems or infrastructure. In the area of dependability, the typical citizens might by now have developed at least a reasonable expectation about a service's availability. In the area of security, no such pre-existing trust concerning system integrity and preservation of privacy and confidentiality can presently be assumed.

Citizens are not well-informed regarding security nor can they easily obtain professional support and advice about security issues.
In a corporate environment or in a government environment, security rules become part of a working contract and are communicated to employees in a structured way. There are usually a comparatively small number of ICT users that are to be addressed and the possibilities to enforce security policies are manifold. The situation of the ordinary citizen is completely different. Although there are a number of relatively well-informed citizens (e.g., cautious people, experts or (self-) trained people), the majority of the citizens cannot be expected to have received special training on security or technology issues. In contrast to a corporate or administrative environment, the citizen usually has no easy access to expert consulting, helpdesk functions or professional advice in security issues either, and often there is a very poor balance between security and usability.

The citizen does not assume any responsibility for security and dependability beyond the personal environment.
From a national government perspective, there is an obligation to assure a Member State's security and dependability and to protect critical infrastructures. The same obligation, limited to the respective business, holds for commercial corporations, companies and especially for operators of critical infrastructures and indirectly also for vendors. The citizens of the Information Society, as far as security in general and the dependability of infrastructure and services specifically are concerned, can simply assume the consumer role. This means the citizen can request security and dependability any time and any place, but is not obliged to contribute in any way to activities that assure this dependability or security.

The Basic Requirements of the Citizen

The European citizen's requirements, therefore, are mainly focused around an individual, personal perception of security and dependability and all its related implications. Individual, personal, democratic, self-determined control is much more important to citizens than the traditional, historic, government-controlled central approach to security and dependability. In the European Information Society, security and dependability concepts must take into account not only central control requirements but also the individual need for security and dependability mechanisms that protect the citizens' privacy and identity. A research framework should pay special attention to areas of security and dependability that do not follow 20th century central command and control approaches, but that instead could lead to an open and trustworthy European Information Society in which the end user is empowered to determine his or her own security and dependability requirements and preferences. This need for self-determination is accompanied by a need for a reliable, dependable infrastructure that such self-determination can be applied to. Processes of the Information Society will be digitized more and more and there needs to be a reliable, failsafe communications environment and infrastructure in place to support these processes. Within this environment, the roles that the citizens can take will be multiple ones: anyone can act as a private person, as an employee, as an economic agent on behalf of an organisation, a national citizen, a citizen of the European Union, a member of any social or political group, or just as an anonymous user of information services.

The citizen's perspective on security and dependability can, therefore, centre on the requirements to protect all the assets of the virtual Information Society that contribute to an individual's personality and existence in real life. These requirements can be illustrated by the following questions:

- The uniqueness of the identity - *Who am I?* and *Who are you?*
- The ability to decide – *What can I choose?* and *What can you choose on my behalf?*

- The privacy of personal knowledge and history – *What do I know?* and *What do you know about me?*
- The ability to act – *What can I do that is right?* and *What can you do wrong?*
- The ability to control – *What can I do to protect myself from risk?* and *How can I manage this risk*?

Consequently, a Security and Dependability Research Framework for Europe's Information Society technologically needs to take into account the electronic equivalents of the above cornerstones of individual existence, namely Digital Identities, Channel Management, Information Privacy and Infrastructure Dependability.

2.3 Organizations' Perspectives on Security and Dependability

Notions of security and dependability have always to be interpreted contextually. For example, an event that is seen as a security lapse or a computer system failure within a particular corporate department may be dealt with so successfully that the corporation as a whole will not regard itself as having a security or dependability problem. Alternatively the problem may not be containable within the department, and higher levels of the corporation may have to become involved in coping with the situation. But if this can be achieved without any stakeholders external to the corporation being affected, the corporation's overall security and dependability will remain intact. Indeed, the very definition of what would constitute a security lapse, or a dependability failure, depends on context - one organization's incident can be another's disaster! In other words corporations today specify their needs for security and dependability as statements that express which risks are acceptable and which risks must be reduced. The capability of dealing with security lapses and dependability failures is hence planned as contingency actions for risks that might or might not have been mitigated.

As indicated earlier, organizations vary greatly regarding their security and dependability needs. However all – from governments, government departments, universities and research organisations, large corporations, NGOs, SMEs, etc., – have, in common with individual citizens, a need to maintain and manage their overall identities, and to try to retain effective ownership of their information assets, and to protect and benefit from their rights. All organizations that rely on others when executing their business processes have therefore a fundamental interest to understand the levels of security and dependability (i.e. "trustworthiness") that their partners exhibit, and thus the type and level of trust which it is reasonable to place on them.

Expressing these security and dependability levels in contracts for business process outsourcing, say, is one of the fundamental problems that are too often neglected. As a consequence, the corresponding service level agreements fail to reflect what is expected. Renegotiating the contract or even moving out of the partnership causes not only costs but also usually leaves the buyer with years of delay. Hence, security and dependability need to be quantified requirements in service level agreements that focus on both liability (the motivator) and design (actions to reduce/eliminate risk by design).

Organizations vary regarding the extent to which they can take effective responsibility for meeting their security and dependability needs, protecting their information assets, etc. And the degree to which they are able to exercise a level of effective control, for example by legal or financial means, over individuals within the organisation, or even outside it, may vary greatly. But it is always unwise for any organization to ignore or deny the realities about citizens outlined in section 2.2 above. Central to the needs of stakeholder individuals in the Information Society are the problems of Digital Identities, Channel Management, Information Privacy and Infrastructure Dependability. They are even more important to the stakeholder organizations, being responsible for their own interests and those of their clients – they apply directly to the organisation's identity management problems, and it is in the best interests of every organisation to see that the needs of individuals in that organisation, or interacting with that organization, are properly provided for.

In regards to being compliant to (IT) regulations European corporations are facing a particular problem. It is currently almost impossible to specify a common European baseline for IT compliance requirements, which means that European corporations (in terms of compliance costs) cannot scale with the market size.

In the above, security and dependability were discussed as though they are always evaluated from a balanced point of view. But it is important to recognize and address the challenges that arise when commercial players explicitly DO NOT WANT other stakeholders to have security, regarding it as being in their interest to prevent this for purposes of control and profit. (An example is when providers of payment cards integrate themselves in commercial transactions between commercial entities instead of incorporating security features such as Digital Cash or other means to reduce risk and enable trustworthy transactions. The service providers thus become the primary source of risk as is seen with identity fraud related to credit cards and data collectors.) In fact, one finds these kinds of potential conflicts when the issues of Empowerment and Dependability are disregarded or omitted for commercial purposes. For example, in DRM, infrastructure channels, and "trusted party" identity schemes, and "trusted computing" products whose goal is less about the protection of the actual user's interests but more about safeguarding the assets of major suppliers of infotainment and functional software.

Such conflict of interest problems have research dimensions (we need to ensure the potential availability of trustworthy solutions), a market dimension (someone needs to bring trustworthy solutions to market) and a regulatory dimension (if the market does not solve security problems themselves, regulatory steps have to be considered). In fact, market and security by design approaches need to be to be the primary focus as moving to regulatory means in security can often lead to unbalanced approaches in which the main risks are left to regulatory protection alone, and situations in which enforcement proves in practice difficult or even impossible. Focussing on ensuring that liability is relocated to those able to deal with the problems is much more effective.

In summary, Empowerment and Dependability are closely interrelated issues, and focussing on Citizen Empowerment in fact helps to address the concerns of all stakeholders.

2.4 Core Concepts and Their Issues

2.4.1 Digital Identities

Related to the aspects of privacy is the citizen's, and in principle every stakeholder's requirement to act in multiple different roles in the Information Society. In contrast to the natural individual identity of a person or an organization, the Information Society is composed of virtual, digital actors that are distinguished by a multitude of identity schemes. Already today, mechanisms such as social security number, bank account number, credit card number, cell phone number(s), business e-mail address, private e-mail address etc. are used by individuals as alternative identifier schemes for different purposes. Sometimes such an identity might quite appropriately lead to a set of persons using the same equipment and services, such that there is no longer a clear one-to-one and not even a one-to-many relationship between digital identities and natural individual identities. Similarly, organizations sometimes need only be identified via their current role, and may be identified differently in different environments. It is, therefore, vital to distinguish between the individual (or other stakeholder), the device, and the communication channel within the overall, integrated picture.

In recent technological research, there have been numerous approaches to the employment of biometrics for security purposes, building on the uniqueness of biometric bodily characteristics and the easy availability of biometric devices. Biometrics has played, and will increasingly play, an important role in crime forensics and in non-repudiation but also for self-protection and proving innocence. What is critically important is to recognise that the goal should not be identification and surveillance but the balance of security needs. For instance biometrics is problematic for use for authentication as the "secret key" is not secret, revocable or unique, – biometrics can be spoofed and victims of identity theft cannot get a new set of biometrics, and using several spoofable biometrics can merely create more "fake security".

Empowerment considerations involve ensuring that the use of biometrics in Identity and key management is based on easily and securely revocable keys such as private biometrics (biometrics locked in mobile tamper-resistant reader-devices) or bio-cryptography (integration of biometric characteristics in revocable cryptography keys) while enabling the use of a plurality of identity schemes. Indeed, empowerment and dependability are not achievable if control is always with someone else and attackers commit identity theft based on faking biometric credentials – an old type of crime that will grow in a world where identity credentials are increasingly used.

Fake identities and identity theft are considered one of the most important issues for the citizen - but in fact are equally important to organizations, such as banks, given the current prevalence of so-called "phishing". In the information society of the future, the breakthrough regarding these issues for transactions and electronic processes will be two-fold: there will be some services that can be used anonymously in community-based or information-retrieval scenarios where there are only loose virtual trust relationships and there are no valuable goods involved. (For example in Blogs or Wikis, such environments can already be seen today.) The other core area of the Information Society contains those electronic processes that have an emphasis on valuable, goods or service transactions. This we typically find in commercial or government-related applications.

For the scenarios as described above, stakeholders may feel a need for validated traceable identities to execute a transaction, such as registering with the tax authority. However, to make such identities useful, they need to be interoperable as well as mutually recognized (e.g., federal government & municipal government). In addition, citizens' and often organizations' privacy must be protected, which may require anonymous and unobservable access, e.g. to a news system, an interactive communication system, or a telephone counselling service. Whilst proper accounting in the case of using pseudonyms must be assured as well. Naturally, this also necessitates a well-balanced handling of contradictory requirements for law enforcement and data protection.

Considering the above is vital insofar as citizens might be willing to provide certain information freely, if benefits are forthcoming (e.g., customer loyalty scheme). In such a scenario, pseudonyms or limited identities must be used that enable citizens to restrict secondary use and control which information they wish to provide it to the merchant, for what purpose and for how long. This is currently not the case for the problems outlined above. Thus, there will be a continuing potential of conflict between merchants and citizens. One potential conflict might be that a citizen feels that the seller only needs to know payment information without their personal details appended. However, the merchant might want things that are not truly necessary from the citizen's viewpoint. In fact, the latter may be willing to provide such information only if he or she can see a clear benefit from giving such information e.g., providing name and postal address to merchant to received ordered goods having no alternative way to achieving this. (Such concerns are perhaps most easily illustrated for citizen and/or consumer stakeholders, but analogous situations can occur, for example, among companies involved in sensitive business transactions.)

2.4.2 Channel Management

The concept of Digital Identity has to be seen as independent of but closely related to that of Communication Channels and Channel Devices.

Identities operate across communication channels and, therefore, need to be separate from such communication channels. At the same time, security and, in particular, accountability, in a channel is closely related to who is using the communication channel rather than the actual channel device being used.

Re-use of the same channel identifiers leads to uncontrollable linkability of identities or transactions, something that presents a serious problem in a digital world. For instance, citizens in their homes have no real protection when using persistent IP addresses. Basic services such as search engines link and profile increasing amounts of data for advertising and other commercial purposes often in databases whose users cross legal borders. If citizens, or any other stakeholders, enter into commercial or government transactions, re-use of communication channel identifiers leads to similar problems.

A key problem is that identifiers collected in one context can be used for attacks in entirely different contexts, so leading to problems such as Distributed Denial of Service attacks, *phishing* attacks or viral attempts to take control of communicating devices for various criminal purposes, with Identity Theft as the most serious problem.

A key and increasingly important focus for secure and dependable ICT must, therefore, be on how to ensure communication channels do not restrict stakeholders', and in particular citizens', security. It is necessary to align this with use of Digital Identities. At the same time, accountability and security against abuse have to be taken into consideration. Issues such as usability, identity credentials and interoperability between identity management and channel operators will continue to grow in importance until suitable solutions have been found and implemented.

2.4.3 Information Privacy

There is a major concern to assure privacy of the individual in particular, though various other categories of stakeholder typically also have privacy concerns. Laws and regulations in the European Union have supported the European approach to data protection, but the citizen might have individual privacy requirements that go beyond these. Data aggregation and data collection are clearly a problem already, and problems such as computer worms, spam mail and phishing have shown how misuse of data that are not necessarily person-related can be highly annoying to the citizen and even block electronic processes that had already established themselves as a habit in business and private life.

The privacy, security and dependability requirements of the citizen are, therefore, much broader than the pure protection of personal data and the continued accessibility of critical services. Any transaction that is performed in the Information Society, any process that is established electronically and any service that is offered over ICT must be trustworthy, i.e. dependable and inherently secure. This can also mean that the citizen can justifiably trust (in the sense of 'depend on') that certain information flows do *not* happen - or by design only happen in a way where citizen retains control. In a privatized, decentralized and dispersed communications environment, the number of central control organisations will significantly decrease. Nevertheless, citizens should be able to determine whom they are willing to trust (for what purposes, and to what extent), but there can also be a large set of parties involved in services and processes, such that a trust decision might be highly complicated or even impossible for citizens to make. Similar concerns also apply between other categories of stakeholder, such as a set of SMEs that have temporarily come together to form a virtual trading organization. The Security and Dependability Research Framework for the future Information Society, therefore, should pay special attention on approaches that provide mechanisms for trust in a heterogeneous, untrustworthy environment.

One should *not* assume that stakeholders do not care about their security merely because they do not understand the consequences of certain actions. The perception of risk can vary significantly from actual risk and, in the short term, convenience may lead some early adopters to make hazardous decisions. But just as we see serious problems with excessive distrust and concern preventing or impeding the take-up of key technologies, e.g. GMO and mobile phone masts, misplaced trust in a system can eventually lead to serious security and dependability failures if such naive trust is used as an excuse to ignore basic individual security.

Data or identity security in critical and value-creating ICT cannot be maintained through regulatory instruments alone, as enforcement is increasingly impossible, impracticable and ineffective. There is a need to move instead to a more integrated approach, incorporating self-protection and built-in security using context-dependent identity and channel management to separate and isolate each stakeholder's different transactions or roles.

2.4.4 The Applications and Services considerations

The service-centric view emerging from the development of service-oriented architectures (SOA) is changing the way IT infrastructure and applications are and will be managed and delivered. This will affect information society's stakeholders in ways that cannot be ignored, and poses challenges in several domains, not only the technological ones.

Applications will utilise components out of different domains of control and will be obeying different policies asking for diverse security and dependability qualities, since they will be offered by a multitude of providers. In fact, contrary to the current situation, components may be owned and operated by many different organisations, and services shared between many consumers. Monolithic perspectives of system security, already challenged in current networked and distributed systems scenarios, must give room to modular and decentralised perspectives representing the reality brought by SOA[2]. and more flexible identity schemes empowering the stakeholders to reduce risk to them.

[2] Whilst SOA brings new perspectives to TSD, it is recognised that SOA does not force any additional framework for more security in composing services and that such a framework has to be introduced explicitly, afterwards. This was a major conclusion at the ESFORS Workshop in September 2006 [8].

In such scenarios, it is not surprising that confidentiality, integrity, availability, and QoS requirements will increase, or at least become more visible in service-level agreements (SLAs), which may be agreed in a dynamic and decentralised way, and may also provide for dynamic variation depending on instantaneous context. However, if nothing is done to tackle this situation, software and services will continue to be offered on a "best effort" basis, rendering the problem of fulfilling SLAs, and in general, of rendering correct and acceptable services, a very difficult one to solve. This amounts, to a great extent, to understanding how organisations can assure themselves, regulators, and customers, that they have appropriate control over their IT.

Risks of the move toward Services

Let us take the service level agreement (SLA) example, since it will be a crucial component of future service oriented architectures. An SLA is a contract. As such, there must be trust between the parties. Since we talk about services, we essentially mean the user trusting the service provider. Obviously, when a provider signs an SLA, it should have the means to fulfil it. The user, on the other hand, should believe the former has those means. But normally, the user is led to believe a more superficial predicate, that 'the provider will fulfil the SLA', regardless of the means. Moreover, details about these means are frequently considered proprietary, and, thus, not available to the user, even if it wanted to assess them.

Imagine the scenario of an application service provider (ASP), who signs an SLA with several clients. The ASP must guarantee certain conditions of quality of service as seen by Internet users, as well as non-functional properties such as security and/or dependability, both of users access, and of the information being stored and manipulated in the servers. The clients may be end clients, or in turn be online service providers, in which case they may themselves sign specific SLAs with their end users, which will reflect the conditions they get in the ASP contract.

Whilst it should directly guarantee that its data centre fulfils what is agreed, the ASP should contract an SLA with the Internet service provider(s), which in turn contract with their raw cable or wireless providers. On the other hand, some of the provisions the ASP contracts with the end user probably depend on properties of infrastructural services transparent to the former, like isolation effectiveness of virtualisation SW/HW, or protection/detection effectiveness of firewall/intrusion detection system compounds.

Such a scenario, which is quite simple, already implies a high degree of uncertainty both in what contributes to fulfilling the end SLA, and in whom to blame when things go wrong. The ASP is the visible tip of the iceberg, and, as things currently go, business practice ends up relying more on muscle (the aforementioned unilateral trust constructions) and legal advisors than on technical arguments and mechanisms, as it should. In a service-oriented architecture world, this can only get worse, and as such, requires methodical research on the methods, architectures and mechanisms to deal with the problem

Society and Policy Considerations

Continued adoption and trust in ICT-based services will depend largely on the user-friendliness of such services. However, 'ordinary' people find themselves having to deal with the well-known plagues of viruses, spam, rootkits and phishing attacks. Existing technologies, in order to protect from such attacks, will introduce costly barriers to the usability of ICT-based services, driving society away from their use. Security technologies that deal directly with people and society must remain user-friendly while being secure.

One complication often found is the combination of multiple trust sources at a country and European level. ICT-based services lack a framework of regulation that determines recommended or mandatory security requirements from a given service. This situation may degrade as we move to SOA, for the reasons already explained, but this may constitute an opportunity to address the problem in a thorough and generic way. The EU has already started to develop rules to secure electronic communications, principally, the *electronic signatures* directive, and *data protection* legislation for electronic communication. We need comprehensive governmental policies for software and services and systems that guarantee interoperation in a secure and dependable way.

2.4.5 Infrastructure Dependability

Empowerment of the stakeholder, and in particular the citizen, is of limited help when there is no environment around to apply it to. Today's Information Society already is heavily dependent on the availability and reliability of infrastructure (e.g. cell phones, wireless hotspots, E-Mail servers and xDSL lines, together with a vast variety of software systems whether running on desktop computers or shared servers). The future Information Society will be even more dependent, as the density of communications infrastructures will increase and new technologies are already on their way. Citizens and other stakeholders therefore need multiple and interoperable ways of access to communications infrastructures and environments provided by different parties. The topics of Critical Infrastructure Protection and Critical Information Infrastructure Protection will partly converge, as even very traditional physical infrastructures (e.g. roads or water supply) will be more and more controlled and managed by information networks. A large share of services will be offered electronically, and many processes that require personal interaction of the citizen today (e.g. renting a DVD, making reservations, identifying him/herself) will look completely different. Although the individual citizen, and stakeholders such as SMEs have limited control over the availability of communications environments and infrastructures, reliable infrastructure and service availability is nevertheless a key concern.

As already discussed, access to digital networks needs to be more related to the context of use rather than to the identification of people or devices in order to reduce the interdependencies and vulnerabilities that will lead to secondary problems due to any interactions.

From the perspective of the various stakeholders, and in particular that of individual citizens, the European Security and Dependability Research Framework, therefore, should address availability, reliability and robustness intensively. In doing so, a holistic approach should be taken that consider both traditional network oriented approaches and new technologies in order to create redundancy and improve service availability by increased interoperability between the different omnipresent, ubiquitous communications technologies of the future. Well-designed redundancy strategies are critical with respect to coping with physical faults and operational accidents, but the problems of possible residual faults, e.g. in complex software, especially faults that constitute exploitable vulnerabilities, require sophisticated fault prevention and removal strategies, as well. Fundamental to the success of such strategies will be the extent to which developers manage to identify and remove undue system complexity. To resolve and make security interoperable in heterogeneous devices and protocols, these essentials security elements should be characterises through a semantic characterisation and definition.

2.4.6 Technologies for security provision

A fundamental requirement is the development of basic security technologies, that include cryptology, multi-modal biometry, secure and dependable software and hardware development, trusted functionality, intrusion detection and prevention, etc. There is a broader need to develop integrated taxonomies, models and tools to capture requirements, support design, verification, integration and validation. It is beyond of the scope of this document to provide an extensive treatment of all these technologies and, therefore, we focus on those considered to be the most fundamental: cryptology, trusted functionality, biometry and the interactions between them.

In order to be effective, the implementation of the techniques provided by cryptology requires a trusted or trustworthy environment – variously referred to as trusted computing, trusted execution, trusted platform, etc. The intention here is not to debate who controls what, but point out the dependency. Quite obviously, conventional cryptography carried out in an untrustworthy environment or agent is of little value[3]. In addition to research in cryptology itself, two related areas, trusted computing and relationships with biometrics, are addressed below.

[3] this is not to deny the possibility of trusted cryptography by untrusted components – hence *conventional*, which may be simply by-passed or spoofed unless further checking were used – but this would then provide some degree of the required trust

Cryptology developments

Cryptology, the science, and cryptography, the practical application of the science, are fundamental to provision of most aspects of security in communications and IT systems– and as a consequence also their dependability.

Work on modern cryptology has been in progress for many years now, delivering results on which much of our information infrastructures are dependent for their current, albeit imperfect, security and dependability. But now, in addition to responses to fundamental issues such as quantum computing, with its potential to invalidate many of our current approaches, the current, and forecast increased, rates of expansion of information flows require new and improved results from the cryptologists.

Numbers of devices are spoken of in billions, and information in terabytes. The implications for cost, performance, simplicity, energy needs, etc. are, to say the least, demanding. In addition to the mathematical science aspects, the requirements for supporting implementation technologies and engineering will have their own challenges when it comes to delivering the goods.

Envisaged developments – ambient intelligence; fully dynamic, heterogeneous, converged communications, GRIDs, etc. – present new challenging applications, which need to be addressed by different or better crypto solutions and methods than the ones we have today.

Some further specific crypto challenges are listed in section 3.9 below.

Trusted functionality

Trusted computing provides cryptographic functionalities in which a trustworthy system can be built, where trustworthiness is defined according to the underlying security policies. Today, one instantiation of these functionalities is provided by a core component called trusted platform module (TPM) and can be used to (i) remotely verify the integrity of a computing platform (attestation and secure booting), (ii) bind secret keys to a specific platform configuration (sealing), (iii) generate secure random numbers (in Hardware), and to (iv) securely store cryptographic keys.

In this context, there are various research issues to be explored:

- *Security model* for the components used on a trusted computing platform such as a TPM: For future developments, it is important to establish an abstract model of these components and their interfaces to be able to analyse the security and cryptographic as well system-related mechanisms that rely on the functionalities of these components.
- *Efficient multiparty computation* using tiny trusted components which have only a limited amount of storage and provide only a few cryptographic functionalities as mentioned above: Many interesting applications like auction and voting may require complex cryptographic protocols or still inefficient computations for their realization depending on the underlying trust model and the security requirements. It is interesting to examine how and to what extent trusted computing can improve the existing solutions.
- *Property-based attestation:* the attestation functionality allows one to verify the configuration of an IT system. This, however, raises privacy problems since one may not be willing to disclose details about the internals of an IT system. In this context, property-based attestation would only require an IT system to prove that it has a configuration of a certain property, *i.e.,* it conforms to a certain (security) policy instead of revealing the configuration itself. Here, one can prove the correctness even if a configuration changes but still obeys the same policy. For this, we need to design efficient cryptographic mechanisms.
- *Maintenance and migration*: using trusted platform modules also require methods and mechanism for transferring complete images (of applications and operating system) from one computing platform to another. Here, one needs to design efficient and secure mechanism to move a complete software image between platforms with different TPMs and different security policies.

Integration of Cryptology with Biometry

Due to its convenience and reliability, use of and research into biometrics is increasing rapidly in recent years. However, privacy and security problems, such as exposure of personal information, identity theft, abuse and counterfeiting of biometrical data and irrevocability, arise. Using cryptology can contribute to effectively protecting biometrical data from these risks. In addition, biometrics provides unique, and possibly irrevocable and incontestable identification of the human being. Integration of cryptology with biometrics can build direct connection between users and their passwords or keys in security system in order to avoid the unpleasant experience of having to remember and use different passwords, risks of sharing and stealing passwords or keys.

Combining cryptology and biometry improves security and convenience of system. However, traditional cryptology cannot apply to biometrics since biometrical data cannot be produced exactly. Research into development of new cryptology for noisy data would then be needed to address this. Techniques such as perceptual hashing and the derivation of keys from biometric data using additional helper data (referenced and/or metadata) are very promising. The combination of biometrics and cryptology with steganography and digital watermarking also offers new opportunities for secure and user-friendly identification protocols that offer better privacy.

There is direct relevance of this area of work to the progress of the management of digital identity discussed in section 2.4.1, above. Some further specific crypto challenges are listed in section 3.9 below.

3 Research areas to be addressed

Introduction

The Advisory Board has taken a bird's-eye view of the results from the Security and Dependability Task Force (STF) and aggregated different challenges around *nine* key areas, extended from the seven areas originally identified by the STF [Annex II]. The results from the Security Task Force add more detail, and provide substantial technological aspects to the Research Framework. The SecurIST Advisory Board recommendations should be seen as high-level advice based on the set of key areas that the Security and Dependability Research Framework should address.

It is clear that information and communication systems, which are key to the functioning of the European Information Society, consist of both technical and non-technical components. The technical components include software and hardware contained in devices, PCs, servers and communications infrastructure. As important as these technical components are, they are not the whole story, and for an information system to function properly, a number of other non-technical factors have to be addressed. These include factors concerning people and their behaviour, such as policies, procedures, best practices, standards (regarding people), risk management approaches, education, training and socio-technical aspects. The Advisory Board believe that it is important for these non-technical factors to be addressed within the Security and Dependability Research Framework.

The nine key areas identified by the Advisory Board are as follows:

1. Empowerment of the various types of Stakeholder, and in particular of Citizens
2. Europe-specific Security and Dependability
3. Infrastructure Reliability and Availability
4. Interoperability
5. Processes for developing more secure and dependable systems
6. Security and Dependability Preservation
7. End user centric Standardization
8. Security and Dependability of Service Oriented Architecture
9. Technologies for security

Each of these areas is outlined below.

3.1 Empowerment of Stakeholders

Stakeholders' and especially citizens' perceptions of security and dependability are and will be heavily influenced by their awareness of the need for security and dependability and their trust or distrust in the services that *Information Society Technologies* deliver. Therefore, user and especially citizen-centric aspects of security and dependability should be a core element of any new security and dependability concept for future information and communications technologies. There is an obvious conflict in paradigms between the traditional central command and control approach to security and a new, user-centric approach. As all central server systems have to open up and integrate with other systems and technologies to enable the benefits of digital society, the classical assumption of large centrally controlled security systems fail with the concentration of risk and growing complexity. Either the access control models will become unmanageable or so high level that surveillance security will become unmanageable and still won't be able to prevent penetration of the increasingly less protective perimeter security. Security has to be semantically enriched and control distributed to protect the central systems security. This results in many questions regarding how to satisfy the differing needs of central organisations such as network operators, governments or law enforcement agencies and simultaneously leave room for self-determined, user centric control of security and dependability.

The Security and Dependability Research Framework should pay special attention to the citizen-centric approach, as under the general threat of terror, there seems to be a temptation to fall back into traditional, historic security concepts based solely on central command and control. Of course, there might well be legacy structures and environments that require central control and for which there is a continuing requirement. But even such environments need to start now to address the new technological challenges of the future Information Society, as they will clearly face competitive technological environments of tomorrow (such as e.g. peer-to-peer communications, self-organised

networks or ad-hoc communications) that do not depend upon central control structures. Consequently, in an ever more complex world, citizens and other end users must be better enabled to control the flow of their personal information. As leaked information is almost impossible to "retrieve", sophisticated mechanisms are needed for anonymity, for user-controlled release and for transfer of information. Could the individual be granted rights and controls equivalent to those sought by commercial organizations through DRM?

Procedural knowledge – describes the user's applied knowledge and skills regarding how to proceed under particular circumstances regarding the protecting of informational assets. Such knowledge is accomplished after some substantial training and practice of the skill has occurred. The saying 'practice makes perfect' applies here whereby more training improves not only the speed but also, most importantly, correctness of the action invoked. As a result, if a certain context occurs as reflected in hands-on training, the appropriate response can occur quickly and without requiring substantial mental processes to do so.

Technical means for controllability – describes the user having access to the necessary tools and resources for being empowered to control the risk for data-veillance and data shadowing. One of the challenges is the increase in number of near-invisible devices as part of the "Internet of things" where Citizens have to be able to control devices without interfaces often operating almost autonomic.

Technical means and procedural knowledge has to be aligned - Education about both security risks and tools to remedy these risks go hand in hand with ensuring empowering tools. Tools without education of usage or understanding of purpose will not work. Understanding of and modelling tools according to human mental modelling of security is also critical as increasing complexity – ceteris paribus – means less ability to manage security risks unless the identity paradigm moves beyond simple identification assuming someone can be "trusted" just because they are identified.

Semantics across different technologies, protocols, devices and security/identity models are critical for users to have manageable security while enabling developers to fulfil their obligations of service level agreements. Applications need to define their security requirements in much more flexible terms as they can often not predict which kind of devices and protocols, they will interface towards. Semantic descriptions and dynamic security resolution with built-in user empowerment will be critical for achieving simultaneous improvement of security and increase flexibility and distribution.

Empowerment represents a careful balance between the user's wish for convenience and simultaneously the need to control who will get access to what information, and when (e.g., interests, online activities and mobile). Moreover, ambient networks provide increased risks for data shadowing while providing greater convenience for users.

The view of identity as such has to move beyond mere Identification towards more nuanced concepts of identity. Government create and enforce a system of basic Identification, but if this is not integrated with empowering user-centric identity management, then National Id turns into systemic security problems and loss of autonomy. The route ahead is not to avoid structured identity and National Id, but to find ways to move beyond SINGLE National Id in both the private and public sector into at least a two-layer model, where on top of trustable Identification is built interoperable and trustworthy identity providing dependable Empowerment of the Citizen with the purpose of protecting BOTH the central systems, the citizen and society interests.

While solutions to the above may be manifold, including but not limited to digital identities, the current trend towards centralising of management and control represents a challenge to empowerment of citizens beyond the digital age. The research needed under this heading will, perhaps more than any other issue discussed in this report, require the *people sciences* as well as technical expertise and insights. Adequate understanding of how existing systems are used, misused, ignored or abandoned requires the expertise from psychologists and sociologists, as well as from the relevant technical areas. Moreover, such understanding is a pre-requisite to the successful development and deployment of future systems that the European stakeholder will trust and use appropriately.

3.2 Europe-specific Security and Dependability

The European Security and Dependability Research Agenda should have a well-defined position on how to align European approaches in comparison to other regions. Only the ability to take into account specific European structures, facts and histories will turn a European Security and Dependability Research Framework from a technologically focused framework that could well have originated from any other region on the globe into a framework that brings real added-value into the European Information Society. The European background that needs to be taken into account includes, but is not limited to, differing technological levels of the 27 Member States, historic trust and distrust relationships, flexible internal and external borders, different languages and different cultures.

The SecurIST Advisory Board, therefore, strongly recommends the pursuit of research into the direction of European Security and Dependability platforms[4]. Such platforms could be based on legislation, processes, practices, software, hardware, knowledge, capabilities or any combination thereof. As certain aspects of security and dependability are out of bounds for European regulation by mandate of the EU treaty [9], of course, the legal basis for any European Security Platform must be carefully validated.

From the stakeholder's perspective, Pan-European Security and Dependability Platforms could provide an added value to being a citizen or other stakeholder of the European Union, in contrast to being the citizen or stakeholder of a Member State only. Any such platforms should in coverage be limited to EU stakeholders but should provide interfaces to approaches from Northern America or Asia: the notion of Security and Dependability Platforms could be seen as an equivalent to existing successful European competitive advantages such as the European Monetary Union [10], the European Economic Union [10] or the European border control system according to the Schengen treaty [11].

An example of a European security and dependability platform (or component) could be, e.g., a legal agreement and technical system recognizing citizen identity cards from all European Member States to serve as a platform for electronic access to government services across Europe. European Security and dependability platforms, of course, are not limited to technological systems but should also comprise skills networks, legal agreements or common awareness campaigns on security and dependability.

The major value of research on European Security and Dependability platforms is threefold: primarily, Europe-specific requirements can be considered more easily than in US or Asian approaches. This will create better solutions from a European perspective and ease the transfer of research results into the European market. Secondly, there will be measurable added value to the European citizen and stakeholder, who will be able to benefit from being a European citizen (by Europe-wide processes, services or agreements). Thirdly, the position of Europe in global competition will be strengthened if European Security and Dependability platforms can be embedded into global technology standards, processes and regulative frameworks.

Establishing European security and dependability platforms will, therefore, provide benefits to European citizens and stakeholders

- on a personal level (for being able to use broader platforms),
- on a European level (due to the pan-European coverage of these platforms), and
- on a global level (due to the global recognition of unified European security and dependability platforms).

3.3 Infrastructure Robustness and Availability

The Information Society is becoming increasingly dependent on ICT infrastructures such as mobile and ubiquitous communications, location based services and the Internet. From the perspective of the stakeholders, the reliability and availability of ICT services will become increasingly important, although the individual, as an end-user, may not wish to pay too much attention to technical background infrastructure.

---

[4] the term *platform* refers here to one or more commonly usable sets of hardware, software, processes, policies, practices, knowledge, capabilities or any combination thereof, and is not supposed to be used in the traditional meaning of "technical system" only.

Converging ICT technologies have started to enable broadband mobile internet access at any time and any place, and many existing legacy processes have been be transferred to electronic platforms and networks. The requirement to address reliability and availability, and indeed overall dependability issues with high priority will, therefore, not be limited to new and converging network technologies and standards. Moreover, it will also be imperative that software and system vendors deliver products, which are perceived as parts of the infrastructure by the citizen, to meet specific dependability responsibilities. Careful adherence to best practice, and to avoiding undue system complexity, will be critical.

Beyond the citizens' direct perspective on ICT, there is an additional demand for reliability and availability facilities and services in the control plane of critical infrastructures that affect the every day life of the citizen. Classical critical infrastructure sectors such as medical, energy, telecommunications, transport, finance, administration and first responders [12] will become an integral part of the Information Society and the borders between the virtual and physical world will disappear. Dependability of critical infrastructure services will depend heavily upon reliable and robust control networks and mechanisms – whether this be for a traffic management system for congested roads or a load distribution mechanism for broadband mobile internet access. Mechanisms to preserve critical infrastructure control that need to be considered must not limit their scope to protection against accidental faults of designers and of operators or cyber crime attacks but cover all scenarios of infrastructure failure, including physical damage by major incidents, catastrophes or terrorist attacks.

3.4 Interoperability

In a secure Information Society, there will not be a homogeneous, standardized technology for communications purposes. Different fixed, mobile and converging technologies will address different requirements from very near field communications via body area networks to broadband broadcast communications across national borders. Security and dependability features and properties of communications systems need to be tailored to the specific needs of the respective communications environment and will ideally be built into the relevant specifications from the beginning. This means that there will be a large set of security and dependability mechanisms, serving similar goals in different environments. The communications landscape will be scattered and dispersed with a very large number of handover points and gateways between technologies. In such an environment, it is of the utmost importance to the end user not to have to cope with a large and complicated set of security and dependability features, but instead to have easy access to the platforms of the Information Society, including an interoperable and integrated security model. The Security and Dependability Research Agenda should respect the current trend towards decentralized and converging communication technologies by addressing especially the area of interoperability and integration of security and dependability mechanisms, technologies and standards. In particular, attention will need to be paid to improved techniques for identifying and removing "security gaps" in highly complex heterogeneous systems. Rather than focusing on "open" standards in meaning of Open Source or Open Processes, focus should be on the semantics of security by establishing and standardising on a meta-level able to cover much wider than merely one security model. The key problem is how to create interoperability between multiple security models for different purposes and enable new kinds of security and identity models for instance incorporating user empowerment. A focus on transparency through verifiable semantic will prove a vital aspect of both knowing and being able to resolve actual security assertions against application security requirements.

3.5 Processes for developing more secure and dependable systems

Ideally, security and dependability should be considered together and treated seamlessly from the first stages of any system design. However, the current reality is different: the development process for information and communications systems today is focused mainly on functional features, whereas security analysis and secure and dependable development are trailing in professionalism and investment in many areas. To avoid increased efforts in adding security and dependability to insecure systems, security and dependability should, where possible, be built into all information and communications systems from the beginning. (This applies whether one is constructing an entirely new system, or one composed out of pre-existing systems.)

This requires a broad approach mainly in the area of software development: threat analysis, risk analysis and the use of appropriate security and dependability architectures should become mandatory in the development process, and software developers are to be educated regarding proper security and dependability design and security and dependability pitfalls. Furthermore, automated software development tools must be provided that include fully or partly automated handling of security and dependability issues as well. Security and dependability in the sense of proper software development covers not only such traditional aspects as authentication and encryption but will rather also aim at proper handling of various specific issues such as e.g. buffer overflow mechanisms, tailoring systems to the end users needs and omitting superfluous functions that might become security and dependability risks. Handling of access rights according to the need-to-know principle and an easy-to-understand management of security and dependability parameters will also be required.

Research on the effectiveness of security and dependability awareness programs with regard to system architects and developers should be done in parallel to see how efficient the measures can be.

The end user perspective is that systems developed according to certain secure and dependable development standards or best practices could achieve a higher level of trust for their stable and reliable security and dependability.

3.6 Security and Dependability Preservation

In contrast to the considerations about availability of services for the citizen described in section 3.3, the increasing complexity of Information and Communications Technologies imposes another challenge for a European Security and Dependability Research Programme: in a more and more complex environment, the stakeholder, and specifically the citizen must preserve his/her security and dependability without needing to become an expert in security and dependability. The increasing number of technological standards and the large number of new technologies, all intertwined, partly overlapping, partly complementing each other and in special cases already converging, make it a special challenge to maintain security and dependability at an adequate level across all components as new systems are introduced. The Information Society will not only use standards that are well-defined, tested and approved by the community but will always be driven by early adopters of new technologies and products. Security and dependability – with a perspective of being as strong as the weakest link in the chain of an interconnected Information Society – is in great danger of falling behind the technological development in the high-speed, short time-to-market scenario sought by the industry.

Preserving security and dependability also means preserving predictability in an uncertain environment with respect to multiple facets of technology: uncertain synchronism, fault model, and even topology. On the other hand, systems are required to fulfil more and more demanding goals, which imply predictability or determinism, e.g. timeliness, resilience, security. Systems, therefore, must be capable of adapting, and they must do so in a more or less predictable and agile/dynamic manner. Moreover, they must retain the good qualities they provided, and above all, any confidence users had in them, mainly with regard to sensitive aspects of information privacy, transaction correctness, etc. The balance of the required predictability and the uncertainty of the environment is a major challenge to be addressed. On the other hand, forward thinking must not be hindered by a lack of security or dependability. The European Information Society of tomorrow will be stronger and more capable with every solid technology platform successfully deployed in the market. GSM in the 1990s has shown that such quantum leaps are possible, and emerging standards, technologies and products with a European origin (e.g. Galileo) might have the opportunity to repeat this success story. Ultimately, a European Security and Dependability Research Agenda should take into account the necessity to maintain security and dependability in an ever more complex and de-centralized technological environment. Current approaches such as high level security and dependability description languages, end-to-end security and dependability, and security and dependability standards already point to one possible direction to address this challenge. Additional approaches are urgently required to provide a stable security and dependability basis for new technologies and to offer seamless, plug-and-play, high level security and dependability to the citizen.

3.7 User centric Standardization

Standardization is one of the cornerstones of a pervasive and secure Information Society of the future. For seamless ubiquitous ICT to become reality, technological interoperability and gateway functions are required. This will only be possible on a basic foundation of standardized or de-facto standardized services and technologies.

Today, standardization is mainly concerned about technological issues and is driven by experts from technology vendors and operators. As the operator role will change in the future due to a trend to more decentralized technologies, the citizen end-user will partly become involved in issues that used to be operators' business before. Therefore, end users should be represented as stakeholders in standardization activities.

Unfortunately, as of today, only very few consumer or end-user representatives have participated in standardization activities (only slowly and on specific occasions, e.g. in the ENISA advisory board or in the SecurIST Advisory Board, first end-user involvement becomes visible). To tailor a more decentralized security and dependability model in the future Information Society to the needs of the citizen, end-user associations and representatives should be more involved in standardization activities. This will require, in all probability, both programmes of awareness raising, and financial assistance aimed at levelling the standardisation playing field.

3.8 Security and Dependability of Service-Oriented Architecture

Further to the research challenges already identified in the previous sections, SOA will further stimulate the need to develop logics and mechanisms for building trust on a given service based on the perceived notion of the actual trustworthiness of several, and sometimes disparate, underlying infrastructure modules. Given the fragmentation that SOA imposes on the classical notion of "system", these relations may well have to develop recursively. Furthermore, given the characteristics of SOA, the above-mentioned relations must include assurance, socio-technical, policy and regulatory aspects.

As ICT systems become more complex and interdependent, it will get ever more difficult to manage security and dependability unless appropriate action is taken. The use of service-oriented architectures (SOA) is intended to increase the business agility that today's organizations need in building federated services; However, at the same time, it is required to provide the visibility and control necessary for underlying horizontal issues such as security and dependability. Additionally, current standards for best practice and security management (e.g., ISO17799/27001) must be adapted to the generalised scenario of outsourcing deals, sub-contractors, etc. expected in an SOA world. Legal, risk and auditing aspects may be important in this endeavour, to study how to share risk/security and dependability information between providers.

We need appropriate models to: configure, change, and assess the security and dependability of aggregated services and information sharing; drive the definition of SLAs; and make assurance cases about their fulfilment. In essence, it is important that we devise mechanisms to establish and maintain trust and manages policy regulations and service contracts such as SLAs, in an SOA context.

Despite the advent of service oriented architectures and the challenges identified above, the quest for seamless integrated security and dependability must continue. Traditional security and dependability protocols alone do not provide seamless and integrated security and dependability across multiple protection domains. New paradigms based on SOA must emerge. The complexity of context-aware privacy and security protection from both the user and the application layer is bound to increase, and needs to be hidden behind appropriate interfaces. Techniques such as virtualisation of personas, devices and services may well be required, as users move across multiple trust and services domains.

Trusting Service Level Agreements in an SOA context

Even with the fairly stable, centralised and visible notion of provider that characterises current business practice, it is already difficult to provide formal technical guarantees about the *capacity* of the infrastructure and supported services to meet given SLAs. Likewise, for services deployed over the Internet, user trust is more of a question of faith, largely based on political/social factors, such as reputation (standing in market), insurance (endorsing responsibility to third parties) or inevitability

(monopoly, public administration) of the provider. The provider in effect says "Trust us, you know us!" or "Trust us, you have no other option!"

One might argue that this situation, awkward as it may be, is unsatisfactory to the users but rewarding to the providers. In fact, this is not true. Providers are the visible face to the end-users, but normally they are, equally, users with respect to other providers, and thus the problem has repercussions throughout the value chain. And unfortunately, the situation will become unsatisfactory, if not unsustainable, to all stakeholders, in an SOA context, if nothing is done to improve the situation. In a service-oriented architecture world, there may be many different participants dealing directly with one another, components may be owned and operated by different and possibly many organisations. In fact, a real application service provider setting may end up being implemented by a multitude of access, Internet, and hosting providers, lying behind as many federated component service providers.

Services will be shared between many consumers; components will obey different and independent security and dependability policies, increasing the risks considerably. If we wish to maintain the traditional approach, we will end up buried under an unmanageable number of SLAs. The most basic reliability theory tells us that failures will be more frequent if we pursue the current "best effort" approach, that SLAs will fail, that the capacity and responsibility (or lack thereof) of service providers will be brought under the spot lights, and that (irresolvable) conflicts will be the rule rather than the exception. In such a deregulated and finely granulated world of components, the fragile *trust* building described earlier risks falling apart.

This brings us back to the crucial problem: users are *forced to place* trust on the services they buy, whereas they should be given *evidence* that allows the *building of* that trust That evidence is very much concerned with the *trustworthiness*, i.e. the *security and dependability,* of the services and obviously, of the infrastructure supporting them. Service providers must provide evidence that they can fulfil the SLAs they sign. This capacity should be auditable by regulators and other authorities. The user should be given means to build trust, either by directly assessing the capacity of the provider, and/or by a transitive relationship with regulating bodies that are trusted by the user, and which can assess the provider's capabilities and capacities.

In an SOA context, all these are research challenges, and the problem has several facets:

- how can users and other stakeholders obtain fixed guarantees about the capacity of providers, as current assurance standards are insufficient for SOA?
- how can organisations assure themselves and regulators that they have appropriate control over their IT to keep it dynamically within agreed parameters?
- how can systems enforce and assess at run-time the individual trustworthiness of components, and be able to include them in trustworthy systems, in particular systems that provide the desired degree of security and dependability against faults, attacks and intrusions?

The future needs to achieve a much closer correspondence between *trust* on the applications as seen by users, and *trustworthiness* of the infrastructure and supporting components. In this future Empowerment will be a key means to enable trustworthiness in ICT, and thereby the means to enable user trust. In essence, this all boils down to the study of the technical (system mechanisms) and legal (standards and regulations) means of guaranteeing, "a service running on S is trusted only to the extent of S's trustworthiness". This is believed to be a key factor of success of business in an SOA world.

Service engineering

There are ongoing requirements for advances in our ability to design and implement trustworthy services, applications, and software infrastructure – fundamental developments in software engineering calling for R&D for:

- construction and composition of secure services;
- secure service engineering and service deployment;
- assessment – verification, validation, etc. – of correctness, security, and dependability of provided services.

3.9 Technologies for security

Behind the foregoing requirements for further R&D in specific key areas is the need for development of the intrinsic technologies – the foundations and building blocks that will support everything else. We can build nice secure models of this and that on our laptops, but when it comes to the real world we need the proper bricks and mortar, steel frameworks, and reinforced concrete. Higher levels of assurance will be sought for the components of the dynamic, heterogeneous networks that will deliver ambient intelligence.

An important challenge in the development of basic technologies is the creation of a common language (taxonomy) and of models and tools to capture requirements, support design, verification, integration and validation of security solutions – the red and green pencils[5] are objects from a distant past.

Two fundamental security technologies that need to be addressed are

- Cryptology – to protect information stored or transmitted outside of a 'home' trusted[6] environment, and even to provide certain trustworthy interfaces within that trusted home;
- Trusted functionality – a generalisation of trusted/trustworthy (footnote 6 still applies) hardware, trusted platform module, micro-code, intimate/kernel software, and basic aspects of operating systems up to some specified API; this can be used to construct a trusted local environment – trusted to do certain specified actions, and only those actions; it can ensure that information is handled by it and within it only as intended; as discussed earlier, the implementation of the cryptographic processes themselves needs this sort of trusted execution environment.

A third area is that of the protocols that utilise the cryptography, as well as manage it. These are interactions between entities to achieve certain security goals. In addition to key-agreement protocols that allow for authentication of entities and for the establishment of key material, cryptographic protocols can achieve much more complex goals: in principle parties can compute any function of information they share while protecting the privacy of their inputs and without the need to trust a single central entity; this is even possible if certain parts of the players are compromised, hence protocols that use these advanced techniques are potentially much more robust than simple protocols in use today.

Work in these areas has been in progress for many years now, delivering a stream of essential results, but the need for billions of ubiquitous, cheaper, smaller, faster, lower power, dependable components implied by the AI vision will place further demands not only on the technology and engineering, but on the underlying physical and mathematical sciences.

Crypto challenges

Specific challenges for cryptology research include:

- *Crypto-everywhere*: software, hardware, and nano-scale implementations will be required as cryptography is deployed as a standard component of all communication and computation layers and – with ambient intelligence (or pervasive computing) – at "every" physical location. Requirements will be for lower cost, higher performance, specific applications, smaller size, low complexity, provable correctness, and low energy consumption.
- *Long-term security*: Many crypto-systems considered robust have been broken after a certain amount of time (between 10-20 years). For instance, most of the hash functions developed before 1993 have been broken. We need to build crypto-system that offer long term security, for example for protecting financial and medical information (medical information such as our

[5] the complete technology support for the first multi-layer silicon and printed circuits

[6] *trusted* in its rather simple-minded interpretation as in TCSEC, etc., rather than the semantic edifices currently under construction, but based on some demonstrable claim to trustworthiness

DNA may be sensitive information with impact on our children, our grandchildren and beyond). In the medium term, we need to be prepared for the eventuality that large quantum computers could be built: this would require an upgrade of most symmetric cryptographic algorithms and a completely new generation of public-key algorithms.

- *Provable security*: cryptography has been very successful in developing security models and security proofs within these models based on a limited set of assumptions but more work is needed to expand this approach to more areas in cryptology; automated tools to assist in developing and checking such proofs seem a promising research direction.
- *Secure implementation*: even if we are able to get theoretically sound cryptographic algorithms and protocols, most of their failures can be found at the implementation level. A design methodology and technical solutions to increase resistance to side channel attacks (power, radiation, timing attacks) and work on secure APIs would be very relevant.
- *Digital rights management*: several techniques such as fingerprinting and watermarking are available and there is a growing interest in this area. However, there is a lack of solid scientific basis (even just openness about techniques used in commercial products) and insufficient academic research.
- *Privacy*: diffusion of sensing, location based services, explosive growth of storage capacity and communication mechanisms, and data mining technologies present a major risk to privacy. The problem lies in the asymmetry of technology: advances in technology make privacy violations much easier, while protecting privacy is complex and delicate (integrated solutions are necessary that work at all layers – physical, network, transport, application). Ease of use plays an important role here too. Advanced cryptographic protocols can bring substantial advances in this area.

Long term security and dependability

Security and dependability issues typically go along with the life cycle of a technology. The trend to first deploy a technology and later fix its problems – typically driven by economic motives – is gradually making way for security by design, resulting in improved security at the beginning of the life cycle. Unfortunately, the security issues of a technology near the end of its lifetime are typically overlooked. The best known example is that of cryptographic keys and algorithms (cf. supra) which may need to offer in some cases security for 50 to 100 years. However, this problem also arises in other areas such as electronic documents. Will it be possible to view current documents 50 years from now and, if so, will it be possible to assert their integrity? Many applications stay in use for much longer than anticipated, but during the extended lifetime they will be functioning in an environment for which they have not been designed, resulting in completely new vulnerabilities and risks. For example, software may be running on a processor that can change its instruction set on the fly or new tools may become available that allow to circumvent or evade security boundaries. In view of the complexity of the challenging security and dependability problems we are facing today, addressing these issues seems to be far beyond the state of the art.

4 Preview – a longer term vision of research in security and dependability

4.1 Overview

In addition to the need for short- to mid-term R&D in the nine key areas identified above, it is also essential that a forward watch be maintained that looks out for the possible developments arising from new or emerging technologies as well as new applications of existing technologies. In other terms, we have to build on top of these nine key areas and provide much longer-term reflections and views on how the research community may address crucial issues related to the evolution of the Information Society in the coming 10 to 20 years ahead. Four future *grand challenges* are given below as examples of where possible (r)evolutionary developments might be anticipated. The purpose of this section is to provide a vision for longer-term cross-disciplinary research in security and dependability.

Digital security and dependability is a discipline that is continuously evolving, with widening deployment of digital (fixed, mobile, wired and wireless) technologies, and their penetration into all aspects of human activity.

The goal of the fast expanding area of Security and Dependability research is to strengthen the secure circulation of data on robust networks, the computations of information on secure and dependable computers within a resilient ambience, promote the dissemination of computer applications and encourage the adoption of digital technologies by the general public, and provide effective means of trust and risk management.

Computing is not a discipline that is governed by the laws of nature[7]. It is a pure creation of the mind, with all its advantages (inventiveness, originality) and faults (errors of strategy, price-fixing, forecasting, specification, design, validation, operational use, etc.).

To grasp the complexity and follow the construction of these digital structures, new abstractions must be created in order to devise new efficient paradigms. It is also necessary to design new models, production tools with new languages, and protocols with modelling, simulation and verification techniques.

In order to construct resilient architectures of large evolutionary systems made up of independent heterogeneous elements that are context aware and fault-tolerant, have adaptive behaviour and take into account mobility, dependability and security, we need the following:

- First, research on **new computing, communication and information models**, taking into account security and dependability, and their enemy, system complexity.
- Second, the **injection of semantics** into these systems, because in a mobile, changing world, information must be validated **locally**. These models must be sometimes discrete, sometimes continuous and sometimes stochastic to envisage the future and explore the environment.
- Third, the creation of **interaction models and knowledge models** so that independent devices can, during their life cycle, learn how best to interact; also **models for creation, acquisition, distribution, sharing of knowledge and trust**.

With all these diverse models, it will be possible to design and build new architectures, new protocols, and new trusted infrastructures.

To carry out such work, we need also to spend efforts on **languages and tools**. This involves the creation of programming and markup languages and tools, interaction languages and tools, in order to inject security and dependability during the design phase. New dependability, security and trust infrastructures with separated instrumentations and processing are required, in order to better grasp the digital activity, and to better understand the validity and the quality of trust. It is also necessary to develop protocols in much more flexible and decentralized networks that will break the monotony and

[7] apart from the fundamental law of engineering: *what can go wrong probably will*

symmetry of network nodes, with algorithms of cooperation, coordination and autonomy, thus resolving issues of scale.

Finally, **assessability** (**verification and validation) techniques** need to be developed.

4.2 Security and Dependability – four Grand Challenges

In this section, four future *grand challenges* that security and dependability science must take up in future years are described as examples of where possible (r)evolution might be anticipated. These challenges are based on a cross-disciplinary perspective and reflect the preparation of appropriate reaction to potential future dark visions and golden opportunities; they are not entirely imaginary, but contain very real possibilities. Underlying R&D directions on which they are based may appear to be FET-like research and beyond, but the outcomes will be very tangible. The security and dependability community needs, therefore, to be vigilant on these possibilities, analysing options for response to consequent opportunities and threats.

Countering vulnerabilities and threats within digital urbanization

The **first grand challenge** is the security and dependability improvement for the expansion and globalization of digital convergence by 2010-2015. In our way to this, we will notably observe three inter-related phenomena: *first*, the boundaries between physical space and cyberspace will start fading away; second, the dependence of citizens and organizations on ICT will increase so that it is crucial to enhance Critical (Information) Infrastructure Protection; and *third*, threats and vulnerabilities will increase while service availability will likely decrease. More specifically, when we consider the figure 99.9…9% of availability for a system or a service, the question is how many 9s are required and how many will be really implemented?

The above can be translated to the following open problems for the security and dependability community to resolve.

- ***how to move from "claustro-security" (closed and ciphered world) to an "agora-security" (open and clear world)?***
- ***how to move from static and standalone activities to a collaborative, network centric architecture vision with full mobility and full interactivity with people and reality?***
- ***how to make the actors' chain proportionally responsible and accountable for malevolent or erroneous actions?***

The evolution is towards ICT infrastructures that are globally interconnected and becoming the economic nervous systems of the modern world. The information society is, thus, becoming ever more complex but also more fragile. On the one hand, cyber terrorism and computer piracy will also set to increase. They will threaten our society and affect the daily lives of our citizens, the management and lives of our enterprises, and the operation of states. On the other hand, a vast number of interdependencies are progressively being built between the different information and communication systems and the various areas of human activity, such as administration, banking, energy, transportation, public health, or defence. New means for reducing the vulnerabilities due to the technical interdependencies are critical calling for security by design, citizen empowering and other ways to ensure damage control to both internal and external stakeholders.

Two trends seem then to emerge:

- Dependence on vulnerable, interdependent, interconnected, complex ICT systems: the information society evolves towards a more interconnected and standardized world. This evolution is characterized by an increasing use of 'open' communication infrastructures, such as the Internet, but also by a widespread use of monoculture software applications. This brings about vulnerability to all kinds of accidental or deliberate incidents and aggression, and their rapid propagation through heterogeneous infrastructures that operate more and more interdependently and under the same standards.
- Real-time resilience and security: The future evolution will involve technical, behavioural, organizational and even psychological changes, as evidenced by the growing dependence of our everyday activities on ICT systems. Companies are said to be agile, with short reaction loop decision cycles and just-in-time procurement cycles. Meanwhile, security also evolves

towards just-in-time (software and antivirus developments). However, its effectiveness will be more and more precarious and there is a need to move towards real time reaction capability to face the growing threats. The security of the dynamic reconfigurability and update of hardware and software at runtime is a major challenge for the years to come.

Overall, the security, dependability, privacy, interoperability, compatibility, administration, and life cycle of these heterogeneous and interdependent infrastructures are open questions.

Duality between digital privacy and collective security: digital dignity and sovereignty

The **second grand challenge** concerns privacy issues of all the players – citizens, groups, enterprises, and states.

There are always two angles of view in terms of security: the point of view of the user who wants to protect himself against the network or some entities there (this is the digital privacy standpoint, with a requirement for the preservation of individual freedom) and the point of view of the network or society, that needs to protect itself against malevolent and irresponsible users (this is the ambient security standpoint, with a requirement for the protection of the community).

The question for the ICT usage is the assurance of digital sovereignty and dignity for citizens and groups. ***how to override the "big Brother" syndrome and the dark security?***

One can thus picture the subtle and tough competition between, on the one hand, the methods designed to preserve a subject's privacy, , ensure empowerment and the legal procedures to watch such subject and, on the other hand, the practices intended to preserve the rest of the world against the potential malevolent or accidental acts of such a subject, and the latter's remedies to find out what means are being implemented to control him and to counter those means. Creating a climate of mutual respect and trust is not detrimental to the setting up of mutual defence cross-procedures. Transparent dialectics should make it possible to negotiate the rules and subscribe to clear and harmonious security policies. Such digital dignity is the price to pay for the democratic values of our civilization but citizen empowerment and means for better balances between accountability in a context and preventing the linkage of outside context represents one example of a way to reduce or eliminate the assumed problem.

Objective and automated Processes

The **third grand challenge** is the obligation to attain a controllable and manageable world of complex digital artefacts by 2015 toward a provable security (predictability of faults, anticipation of threats).

The challenge is the measurability issue:

- ***how to inject regular, quantitative techniques and engineering to make the field truly scientific?***

Beyond the Horizon: a new convergence

The **fourth grand challenge** is the preparation of a new convergence at a horizon of 2020 and beyond, which is the bio-nano-info-quantum "galaxy".

In this perspective, we may observe the decline of the present IP/3G/Google Age by 2010-2015 and perceive a disruptive appearance of new infrastructures by 2015. Currently envisaged IP may not be sufficient to support the next generation of wireless infrastructures (2015). The 3G/post-3G will likely be replaced by more open and interoperable infrastructures (2010-2015), and the content galaxy (information, multimedia, programs) will likely be replaced by new services (2015). During the next twenty years, we will partake in a long digital twilight and a novel re-emergence of "analogue" systems with combinations of atomic engines (nanotechnology) and/or living cells (bio-geno-technologies).

The emergence of bio-nano-infospheres will create a (4D+1D) multidimensional intelligence and disruptive mechanisms for the 21st century. A full new interface for security and dependability between those four universes (living + physical + digital + quantum) will have to be invented.

The big question will then be: ***how to protect the interfaces and to attain and maintain a security continuum?***

References

[1] European Commission's Regulation 2005/516 of April 22, 2005.

[2] http://www.enisa.eu.int/Engberg, S., Workshop presentation at Security Task Force Workshop 19th April 2005. http://www.securitytaskforce.org/dmdocs/workshop2/stephan_engberg.pdf Additional: Trust In the Net Workshop (09 Feb. 2006) report available at http://www.egov2006.gv.at/Reports/Report_Trust_in_the_Net_Vienna_09_FEB_06.pdf

[4] SecurIST Deliverable, D3.2 Validation Workshops report (Non - public version), November 2005.

[5] Veríssimo, P. E., and Neves, N. F., and Correia, M. P.: Intrusion-Tolerant Architectures: Concepts and Design. In: Architecting Dependable Systems. Springer-Verlag LNCS 2677 (2003). Extended in Technical Report DI/FCUL TR03-5, Department of Informatics, University of Lisboa (2003). http://www.navigators.di.fc.ul.pt/it/index.htm

[6] http:// www.itu.int/internetofthings

[7] SecurIST Deliverable, D3.1 ICT Security & Dependability Research beyond 2010 Initial strategy (Non - public version), October 2005

[8] ESFORS September 2006 Workshop report http://www.esfors.org/downloads/ESFORS_Workshop_200609_Report_v1.3.pdf

[9] http://europa.eu.int/eur-lex/en/treaties/dat/treaties_en.pdf; Additional: http://europa.eu.int/eur-lex/en/treaties/selected/livre106.html (Article 23)

[10] http://www.absoluteastronomy.com/reference/economic_and_monetary_union

[11] http://en.wikipedia.org/wiki/Schengen_Agreement.

[12] EU: CI2RCO Project www.ci2rco.org; European CIIP Newsletter - http://www.ci2rco.org/ecn/European%20CIIP%20Newsletter%20No%201.pdf; Additional references: US Department of Homeland Security report http://www.whitehouse.gov/homeland/book/sect3-3.pdf, page 30
Canada: http://ww3.psepc-sppcc.gc.ca/critical/nciap/nci_sector1_e.asp
UK (MI5) http://www.mi5.gov.uk/output/Page76.html
Germany (German only): http://www.bsi.de/fachthem/kritis/KRITIS_Einfuehrung.pdf).
and many others.

Part II - Glossary

Glossary

This glossary defines the various concepts that come into play when addressing the:

- dependability and
- security of

computing and communication systems. Uncertainties about system boundaries, language and cultural as well as legal matters make the definition of such concepts quite difficult indeed.

On top of this comes the very complexity of systems, and of any specifications they have, making it again difficult to define and describe what one is talking about.

Finally, the determination of possible causes or consequences of failure can be a very subtle process, and there are (fallible) provisions for preventing faults from causing failures.

This glossary was launched by the Advisory Board of the Security Task Force (www.SecurityTaskForce.org)

A major challenge with most attempts at such a set of definitions is to avoid imprecision and circularity - in essence the definitions provided in this glossary take as their main starting point the terms "system" and "judgment", for which ordinary dictionary definitions will suffice.

This glossary benefitted from previous work done in this area by:

- Avizienis, A., Laprie, J.-C., Randell, B. and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, Volume 1, Issue 1, pp 11-33.
- Gattiker, Urs. E. (2004). Information security dictionary. Defining the terms that define security for e-business, internet, information and wireless technology. Boston/Heidelberg: Kluwer Academic Publishers & Springer Science (ISBN 1-4020-7889-7).

Finally, this glossary provides readers with definitions as they apply to the work of the SecurIST Advisory Board's policy paper entitled:

- SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework that can also be downloaded here: http://casescontact.org/euist_view.php?newsID=3919

This glossary can also be searched online and printed at:
http://cytrap.org/RiskIT/mod/glossary/view.php?id=7&mode=letter&hook=ALL

Access control: is the enforcement of specified authorization rules that require the:

- positive identification of users,
- the system, or
- data

that can be accessed.

Ambient network: Ambient is the immediately surrounding area. The term ambient defines the area the individual is currently located at whereby the surroundings act as a natural interface to access through the network a universe of integrated intelligent services. This provides the opportunity for access to any network, including mobile personal networks, through instant establishment of inter-network agreements. To illustrate, the individual is being handed off from the wireless operator's network to the coffee shop's (schools, office building's) private network until she leaves the latter. Then she will be handed off again to the wireless operator's network.

Accordingly, the term ambient network refers to the presence of a digital environment that is:

- sensitive,
- adaptive, and
- responsive

to the presence of people. An ambient network can thus be characterized by the following basic elements:

- ubiquity,
- transparency, and
- intelligence.

For an ambient network to succeed it must be both, scalable and adaptable. It must also encompass:

- hardware that is stream-efficient to provide computational resources that are both energy-efficient (see limitations of energy charge for today's smartphone) and powerful for a variety of computational tasks, and
- software and protocols for providing flexibility and spontaneity, such as by supporting smooth vertical hand-offs among communication technologies - from one mobile tower to a WiMax antenna whilst travelling on a train. This also requires that services and software objects must be named by intent, for instance, ‘the nearest printer’ that could be at the coffee shop one is spending time at, rather than by network address that connects to one's home or office printer.

Authentication: Any process by which a system verifies the identity of a user or system that wishes to access it.

Authorization: the process of granting a:

- person,
- computer process, or
- device

access to certain information, services, or functionality.
Authorization is in the context of authentication of the user, process or device requesting access. Once a user's, system's or process' identity has been authenticated or verified, the user or process may be then be authorized to:

- perform different activities (e.g., read database only - no authorization to either add or change data); and be
- granted different levels of access (e.g., view data from last 2 months of customers in region A only); and to
- perform data alterations (e.g., change or add database entries) if need be.

Availability: can be defined as readiness for correct service (see also dependability)

Confidentiality: is the property that information is not made available or disclosed to unauthorized individuals, entities or processes.

Context: the context of a particular use of a system relates to the then current state of relevant aspects of the system's environment. (These could for example include the identity and intentions of the system user.)

Put slightly differently, context is the framework within which a specific situation occurs. The context frequently stipulates how a specific experience, or event is being interpreted.

Critical fleet of infrastructures: The term infrastucture denotes the shared services and facilities that support the functioning of, for example, a system, a community or a country. Critical infrastuctures are infrastuctures on which the entire population of a major organzation, an entire country or a set of countries are highly dependent. These include:

- roads,
- railroads,
- electric and gas supply,
- water,
- sewage,
- telecommunication networks.

Data shadow: represents the trackable data that a citizen creates by using technologies, such as credit cards, cellphone, and the internet (see also Dataveillance).

Data spill: is an accidental transmission or display of private online data to a third party. Such a spill means that we are increasingly susceptible to Dataveillance.

Dataveillance: is the ability to monitor people's activities by studying their data shadows. A synonym that is not as popular, but rolls off the tongue a little better, is consumer espionage.

Decentralization: includes three distinct types of responsibility transfer to people, systems and/or devices and what is called:

1. devolution,
2. deconcentration, and
3. delegation.

Devolution is the permanent-legal, constitutional or technical-transfer of decision-making authority from a higher level of the organization, system or device to a lower level (e.g., having one's communication device being 'handed over' from the network operator to the restaurant's ambient network)

Deconcentration is the transfer of decision-making authority from higher to lower levels of the organization or technical infrastructure within the same level of network. So whilst travelling on a train, the communication device is handed over from tne network operator's 'network' to the 'control' device on the train car and/or the train itself.

Delegation is the assignment of decision-making authority to other systems, providers or organizations (e.g., due to outsourcing customer data from subscribers is handled by another system or organization).
The ever increasing use of information infrastructures involving the use of ambient networks necessitates the decentralization of various processes such as authorization. Each sub-system or infrastructure becomes dependent upon the proper functioning of the devolution, deconcentration and delegation of responsibilities (e.g., handing over of device to another ambient network, appropriate billing).

Denial-of-service: represents an attack that causes a system to be damaged, whereby the damage is sufficient to make at least one of the services offered by that system unavailable.

Dependability: is the ability to avoid failures that are more frequent or more severe than is acceptable. It should be noted that a system or service can fail in many different ways. For instance, it can produce:

- wrong results,
- results that are too late,
- no results at all, and
- results (or absence of results) that cause catastrophes.

Note that from different viewpoints, there can be different judgements as to what constitutes a failure, and hence what levels and types of dependability have been, or are predicted to be, achieved.

One can classify such types of failure and arrive at an identification of a set of attributes (or characteristics) of dependability, the main ones of which are:

- availability,"readiness for correct service,"
- reliability - "continuity of correct service,"
- safety - "absence of catastrophic consequences on the user(s) and the environment,"
- integrity - "absence of improper system alterations,"
- maintainability - "ability to undergo modifications, and repairs."

Also check **Security**.

Dependence: the dependence of system A on system B is the extent to which system A's dependability and security is (or would be) affected by that of System B.

Thus system A:

- is totally *independent* of System B if it cannot be affected in any way by System B and its failures - as well as
- is totally *dependent* on System B if:
  i. any failure of B causes A to fail, and
  ii. A has no other failures.

There can be different types of dependence, such as a user may depend:

- critically on the security of a system (e.g., to maintain the confidentiality of certain information) but perhaps:
- somewhat less critically on its availability

Also these levels of dependence may vary with time.

Digital dignity: see Empowerment

Empowerment: is a concept that includes the citizen's:

- ability (competence, power, education, inclusion),
- capability (tools, ressources and transparancy) and
- accessability (to systems and data

with regard to the control of information,identity and digital assets (e.g., personal data - customer profile or medical data).
This includes control of transformation processes regarding digital assets (e.g., alterations, transfer and addition of data to medical or cell phone / smartphone records or a credit card customer profile).
Here it is important to separate between exclusive power and mere influence on records one might can have power to add, but only influence to alter or delete data as the data set can have been copied or backed up.
With pseudonymity or anonymity, the citizen can have power to eliminate the linkage between data sets and his person. This can occur even after personal data has been added to a profile. It thereby follows that the citizen to have controllability to have empowerment has to use some sort of pseudonymity or anonymity.
Without controllability, however, placing one's trust on a system's dependability or security is an act of faith (see also definitions provided for trus, dependability & security). Most standard communication protocols today do not abide to principles of empowerment as they lacking with regard to both controllability and accessibility.

BTW. Achieving anonymity or pseudonymity is difficult if, for example, each

- Xerox or Canon printer can be tracked or every
- Dell computer is being fingerprinted and tracked anywhere and everywhere on the internet,

thereby making efforts at hiding one's IP address or surfing anonymously futile. If nothing else, the original owner who purchased the equipment can probably be found. In turn, tracking down the current owner of the equipment should not be too difficult. Achieving anonymity is becoming ever harder as technology is being increasingly used to identify equipment, humans and/or locations.

Finally, *Dataveillance* is a big threat to empowerment because unless citizens can control what is being done with such information, citizens' privacy cannot be protected.

Environment: During use, a system interacts with its environment and may be adversely affected by faults originating in it. This environment consists of the following elements:

- the physical world and the system infrastructure, as well as
- administrators, users, provider, and intruders.

These elements, individually and collectively, can all be regarded as systems.
The environment defines, from moment to moment, the evolving context in which the system is operating.

Error: can be described as the part of the total state of a system that may lead to its subsequent service failure.
An example would be a corrupted disk block, which might however either be overwritten without being used, or be outvoted by other correct copies of the block, so failure is not necessarily inevitable. Another example could be a set of incorrect instructions in a program, which if executed might lead to system failure.
The set of three terms (error, fault and failure) leads to the notion of a fundamental chain, expressing how a fault (or faults) may lead to one or more errors, which may lead to a system failure. Such a failure may itself constitute a fault in some other system. This might be the enclosing system, or a separate system that is being interacted with, or a system that is being constructed (e.g. a mistake made by a design team, i.e. a design failure, can result in an error consituting a vulnerability in the designed software, which could be one of the faults, i.e. contributory causes of the software system suffering a security failure.)
There are a large number of different terms in use for these concepts, but proper understanding requires a careful distinction be made between three essentially different concepts that are expressed by the three terms error (a state), failure (an event) and fault (a cause), whatever words are actually used for them.
See also fundamental chain.

Failure: is an event that occurs when a system's delivered service deviates from the correct service. Failures can be subjective and disputable, thereby possibly necessitating judgment to identify and characterize, and may be recognized only after their occurrence, for instance via their consequences. Failure is in fact a central, and very slippery, concept that thus in principle always concerns three systems:

1. the failing system,
2. the system that is using it (equivalently, the system's environment), and
3. the judgment system that is determining whether the service received by the using system is correct - though the user and judge may well be one and the same system.

Again in principle, *judgment is needed* to identify:

i. system boundaries,
ii. failures and
iii. faults.

Moreover, such judgments can vary over time, even from a given judgment system, leave alone between different judgment systems. And a judgment system may itself fail (through delivering an incorrect verdict, an occurrence that, for example, the hierarchical set of legal courts is set up to dealt with). Nevertheless, many situations will be so straightforward that the fact that judgment is involved will hardly be noticed; often situations may be readily resolved with the aid of a (fully detailed and agreed) specification - it is the other situations that are the problem.
The concept of failure is central to such definitions as:

- security
- dependability,and
- trust

Different stakeholders can have different views (e.g., commercial, legal or technical judgments) as to what should be judged a failure, and hence on the (types of) dependability and/or security of a system (or a service).

Failure is one of three conceptually very distinct threats to dependability (and security), the others being:

- error, and
- fault.

Finally, a failure may be recognized as such only after its occurrence, for instance via its consequences. Accordingly, failures can be *subjective and disputable*, thereby possibly necessitating formal means of judgment to identify and characterize them.

Fault: is "the adjudged or hypothesized cause of an error".
Very often there will be multiple causes, such as a software bug that constitutes a vulnerability, together with a hacker who finds a means of exploiting this vulnerability.
A fault is active when it causes an error, otherwise it is dormant.
There are many different types of fault, which can be classified in a number of ways, including:

- System boundaries - internal or external
- Phenomenological cause: natural or human made
- Dimension: hardware or software
- Objective: malicious or non-malicious
- Intent: Deliberate or Non-deliberate (i.e. a product of unawareness)
- Capability: Accidental or Incompetent
- Persistence: Permanent of transient

Another set of (overlapping) classes of fault are:

- development faults: these include all fault classes occurring during development;
- physical faults: these include all fault classes that affect hardware;
- interaction faults: these include all external faults.

Specifications, being themselves a form of system, can suffer from many different types of fault - two particular kinds are omission faults and commission faults (such as misinterpretations, unwarranted assumptions, inconsistencies, typographical mistakes).

The achievement of dependability and security requires addressing:

1. fault prevention,
2. fault tolerance,
3. fault removal, and
4. fault forecasing

as also defined in this glossary.
See also fundamental chain.

Fault forecasting: can be defined as estimating the:

a. present number,
b. future incidence, and the
c. likely consequences of faults

An example for getting the above numbers would be the applying of statistical methods and statistical testing of data.

Fault removal and fault forecasting aim to reach confidence in that ability.

Fault prevention: can be defined as preventing the occurrence or introduction of faults as exemplified in formal verification.
Fault prevention and fault tolerance aim to provide the ability to deliver a service that can be trusted.

Fault removal: encompasses efforts for reducing the number and severity of faults as illustrated by means such as:

- debugging, and
- preventive maintenance.

Fault removal and fault forecasting aim to reach confidence in a system's ability to deliver a service that can be trusted.

Fault tolerance: can be described the means to avoid service failures in the presence of faults, using such tools as:

- firewalls, and
- replicated servers.

Fault prevention and fault tolerance aim to provide the ability to deliver a service that can be trusted.

Fundamental chain: The set of three terms (error, fault and failure) leads to the notion of a fundamental chain, expressing how a fault (or faults) may lead to one or more errors, which may lead to a system failure. Such a failure may itself constitute a fault in some other system. This might be the enclosing system, or a separate system that is being interacted with, or a system that is being constructed (e.g. a mistake made by a design team, i.e. a design failure, can result in an error consituting a vulnerability in the designed software, which could be one of the faults, i.e. contributory causes of the software system suffering a security failure.)

There are a large number of different terms in use for these concepts. However, proper understanding requires a careful distinction be made between the three essentially different concepts that are expressed by the three terms error (a state), failure (an event) and fault (a cause), whatever words are actually used for these concepts.

Integrity: is the property that data or information have not been altered or destroyed in an unauthorized manner.

Maintainability: is the system's ability to undergo modifications, and repairs (see also dependability).

Maintenance: following common usage, includes not only repairs, but also all modifications of the system that take place after the system is first placed in service.

The distinction between fault tolerance and maintenance is that maintenance involves the participation of an external agent, such as:

- a repairman,
- test equipment, and
- remote reloading of software.

Repair is part of fault removal and can be seen as a fault tolerance activity within a larger system that includes the system being repaired and the people and other systems that perform such repairs.

Malicious fault: A fault that was introduced with the intention or desire to do evil or cause injury to another

Malware: Software that embodies malicious intent (see also Malicious fault).

Non-visible and inconspicuous infrastructure: is pervasive infrastructure that may be invisible to the individual or else could be worn by the individual, such as, involving devices or equipment for:

- location,
- communication

Phishing: This describes the case when an attacker sends you an e-mail falsely claiming to be a legitimate business in order to trick you into giving away your account information, such as:

- passwords,
- gender,
- mailing address, and
- birthdate,

mostly. These attacks prey on the gullibility of people.

Phishing distinguishes itself from a worm or virus attack, because the latter two exploit vulnerabilities in computer code. In phishing, the victims are people who get e-mails and visit websites, and generally believe that these e-mails and websites are legitimate.

The real crime with phishing is an ancient one: financial fraud. Having the information the malicious user then tries to initiate transactions or purchases using the information obtained from the trusting and unsuspecting individual.

Trend. The newest variant, called "*spear phishing*," involves individually targeted and personalized email messages that are even harder to detect.

For more information including some nifty tools for fighting off phishing attacks please visit here:
CT210012: UPDATE 2 - Microsoft tool tested - Yes Virginia - phishing attacks are on the rise and getting meaner - we tell you how to surf safer.

Privacy: in the European Union, privacy is generally defined as a right of self-determination, namely, the the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others.
Regulation addressing this is such as:

- European Data Protection Directive that is rooted in the concept of consent, while
- California SB 1386 is putting a price tag on privacy, and
- the U.S. Federal Trade Commission has shown a fine is much more expensive than its price tag, considering the loss in stock value ChoicePoint shareholders had to absorb in 2006-01.

An alternative definition considers privacy as a concept that represents a person's interest in sustaining a 'personal space', whereby he or she enjoys freedom from interference by other people and organizations.
Protecting one's privacy or personal space requires certain security measures to safeguard personal data, as well as specific privacy technologies that enable the individual to exercise a substantial degree of control over his or her data and their use.
However, an ever more decentralized use of technology is making the administering and centralizing of information ever more unlikely, while making faith in security ever more difficult. Moreover, unless privacy regulation is enforced quite striclty, its usefulness must be questioned. However, if beyond fines failing to address security properly starts to cost shareholders dearly, executives will begin to care as the ChoicePoint case illustrates.

See also *Data shadow*.

Reliability: is continuity of correct service (see also dependability).

Safety: is the absence of catastrophic consequences on the user(s) and the environment (see also dependability).

Secure & dependable computing: represents a system that:

1. combines the characteristics of confidentiality (i.e., the absence of unauthorized disclosure of information), allied with availability to conduct authorized actions, empowerment for stakeholders to control risk to them and also integrity (i.e. the absence of unauthorized system alterations) (i.e. Security); and
2. is able to avoid failures that are more frequent or more severe than is acceptable (i.e. Dependability).

Secure & dependable computing are built upon the concepts of Security and Dependability. The latter two are distinct but related and sometimes described using the term Trustworthiness to denote their combination.

See also *Security*, *Dependability*, *Trustworthiness*

Security: can be defined as the combined characteristics of:

- confidentiality (i.e., the absence of unauthorized disclosure of information), allied with
- availability to conduct authorized actions, and also
- integrity (i.e. the absence of unauthorized system alterations)

Security concerns largely centre on problems caused by deliberate malicious actions. Examples are such as those resulting in:

- intrusions,
- viruses and
- Trojan horses,

rather than on accidental faults, such as:

- operational hardware faults or
- residual software design faults.

Security and dependability overlap and are both required. For example, component systems that are intended to provide security facilities, such as, authentication or encryption, to some larger system should do so dependably - and the security of the overall system will depend on them doing so. Unfortunately, and most confusingly, the terms dependability and security are sometimes used interchangeably or, else, either term is used to imply their combination. In fact, because security and dependability are distinct but related and somewhat overlapping concepts, the term trustworthiness is being increasingly used, especially in the United States, to denote their combination.

Service: An entity that interacts with other entities, i.e., other systems, including:

- hardware,
- software,
- humans or users, and also the
- physical world with its natural phenomena.

These other systems or entities are the environment of the given system.
An important class of system, sometimes termed "computer-based systems", involves humans as, in effect system components.
Such "human component systems" can:

A. fail, and thus from the viewpoint of the larger system be regarded as faults, or else can
B. contribute to the dependability of the overall system by helping to tolerate faults elsewhere in it.

Service failure: this term is often just termed a failure. In our definition it is a transition from correct service to incorrect service. That means to not implementing the system function.
The period of delivery of incorrect service is a service outage.
The transition from incorrect service to correct service is a service restoration.
The deviation from correct service may assume different forms that are called service failure modes and are ranked according to failure severities. (See under Failure for the judgment issues underlying the recognition of failures.)

Socio-technical aspects: The socio-technical approach has at its core at the:

1. technical sybsystem that comprises the devices, tools and techniques needed to transform inputs into outputs in a way which enhances the economic performance of the organization;
2. social system comprises the employees (at all levels) and the knowledge, skills, attitudes, values and needs they bring to the work environment as well as the reward system and authority structures that exist in the organization, and
3. environmental subsystems that encompass the wider reach of the organization by including customers, suppliers, and the rules and regulations, formal and informal, which govern the relations of the organization to society at large.

Hence, to optimize systems requires a fit whereby the design process must be aiming at the joint optimization of the subsystems.
Moreover, redesign must seek out the impact each subsystem has on the other and design must aim to achieve superior results by ensuring that all the subsystems are working in harmony.
The organizational systems will maximise performance only if the interdependency of these subsystems is explicitly recognised.

Sociotechnical design: produces information systems that blend technical efficiency with sensitivity to cultural, regulatory, organizational and human needs.

Specification: is a document that attempts to define the intended function of a system, and hence what would constitute failures of a system. The dependability & security specification of a system must include the requirements for the attributes in terms of the acceptable frequency and severity of service failures for specified classes of faults and a given use environment.
Such documents are of great importance in guiding the design of a system, and in helping to establish whether system failures have occurred, but in practice can themselves contain errors, so that what might need to be repaired is the specification instead of, or as well as, the system.

Stakeholders: encompases many parties that have vested interests, including but not limited to:

- individuals, as well as
- organizations (e.g., corporates, NGOs, government departments & Member States).

System boundary: can be used to describe the common frontier between the system and its environment.

Threat: can be defined as an action or event that might prejudice security and dependability.
A distinction can be made between

1. design-based, and
2. blended threats.

The former is a profile of the type, composition, and capabilities of an adversary and can be used as a basis for designing safeguards systems to protect against faults or disasters due to acts of sabotage and theft.
A blended threat is a computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods. An example could be the use of both viruses and worms, while also taking advantage of vulnerabilities in computers, networks, or other physical systems to harm trustworthiness.
There are three conceptually very distinct threats to trustworthiness (i.e. security and dependability) namely:

- error,
- failure, and
- fault.

Faults might again increase the probability or risk that a threat is being realized.

Trust: accepted dependence.
In dictionaries, however, trust is defined as something similar to assured reliance on the

- character,
- ability,
- strength, or
- truth

of someone or something -- as well as a person or party in which confidence is placed. In fact, a thesaurus will probably indicate that Trust and Confidence are synonymous.
However, defining trust as accepted dependence in IT security and new media also entails different types of dependence. Accordingly, a user can trust/accept to be dependent on just some aspects of a system's dependability and security. To illustrate, the user might trust a system with regard to its ability to ensure the integrity of financial data that it holds. However, the user could possibly very appropriately be unwilling to trust and depend on the system being continuously available.
Also, these levels of dependence may vary with time, so the user's trust may, or at least should, also vary.
In principle for A to trust B involves a judgment by or on behalf of A regarding B's dependability and/or security, and how this might affect A. The factors that could influence this judgment include:

1. the perceived credibility of any claims regarding B's security and dependability - this could be related to the objective credibility of the product offered, such as the expectancy that the customer can rely on the seller’s word or written statement about the security product’s or service’s performance,
2. the perceived benevolence associated with system B, which means the system provider’s interest in the customer or client’s welfare and motivation to seek a joint gain and, finally,
3. A's perception of its dependence, whereby the user or client has to judge if the level of credibility and benevolence results in a level of dependence that is acceptable (of course this is related to risk perception)

Such a judgment (made by or on behalf of A) about B (e.g., the system) is possibly explicit, and even laid down in a contract between A and B.
However, it is also feasible that the judgment and the consequent acceptance decision are only implicit, even unthinking. Indeed the acceptance might even be unwilling in a situation where A has no alternative option but to put its trust in B. Thus to the extent that A trusts B, it need not assume responsibility for (i.e. attempt to provide means of tolerating) B's failures.
The judgment about B also represents the willingness of A to accept perceived risk (to get a perceived benefit) within a perceived context whose outcome may result in some level of harm to A..
Of importance is also to be aware that trust is a continuum and not a dichotomy, whereby as a limited

resource, trust always implies some risk of failure that results in harm of the party that put trust into something such as a system or a process. Moreover, there may be differing forms of trust, corresponding to different forms of security and dependability.

Trustworthiness: is a synonym for the *dependability* and *security*
so as to retain the distinction that must be made between dependability and security, and to avoid having to use the phrase repeatedly (see also Trust).
Trusworthiness (i.e. security and dependability) must be taken together and seamlessly beginning with the design of new technology or systems with respect to the risk mitigation of all stakeholders.
Challenge: Systems must be capable of adapting to assure trustworthiness at an acceptable level for various stakeholders (e.g., operator, user and society).
However, they must do so in a more or less predictable and agile/dynamic manner.

Trustworthy computing: synonymous with "*secure and dependable computing*."

Vulnerability: an internal fault that enables an external fault to harm the system. The prior presence of such a fault is necessary for an external fault to cause an error, and possibly subsequent failure(s). To illustrate, a programmer may have failed, and generated code that is capable under some circumstances of causing a buffer overflow error - this is a dormant fault until it is activated through the efforts of some external attacker.

Annex I – Advisory Board Members List

Annex I – Advisory Board Members List

Name	Organisation
Stephan Lechner Chair	Siemens AG
Urs E. Gattiker Vice-Chair	CyTRAP Labs, & CASESContact
Tobias Christen	Zurich Financial Services
Francois Cosquer	Alcatel
Stephan Engberg	Open Business Innovation
Sonia Heemstra de Groot	Twente Institute for Wireless&Mobile Communications
Bart Preneel	Katholieke Universiteit Leuven
Brian Randell	University of Newcastle
Kai Rannenberg	Goethe University Frankfurt
Michel Riguidel	ENST
Alan Stanley	Information Security Forum
Paulo Verissimo	Faculdade de Ciências da Universidade de Lisboa
Andreas Wespi	IBM, Zurich

Ex-officio members (non-voting) and Administration

Name	Organisation
Jim Clarke	Waterford Institute of Technology
Willie Donnelly	Waterford Institute of Technology
Zeta Dooly	Waterford Institute of Technology
Keith Howker	Vodafone

Annex II – STF Challenges Aggregated to Seven Key Focus areas.

Annex II – STF Challenges Aggregated to Seven Key Focus areas

Legend	
1	Primary
2	Secondary
	EU Specific needs is shaded as it is assumed revelant to all challenges

No.	Initiative	STF Challenge	Empowerment	EU specific needs	Availability	Interoperability	Development	Preservation	User-centric standards
1	AS - Applic.	Application Security process in the development	2				1		
2	AS - Applic.	Security in Web enabled environment						1	2
3	AS - Applic.	Secure Open Source					1	2	
4	IIS - Internet	New security and trust on the internet					1		
5	IIS - Internet	Secure Home Internet connectivitiy			1	1			
6	IIS - Internet	GRID security			1				
7	IIS - Internet	Secure Code Development					1		
8	IIS - Internet	Redesign / handling existing SOA					2	1	
9	IP - Privacy	Data Correlation	2		2	2	1	1	1
10	IP - Privacy	Identity compatibility	1		1	1	1	2	1
11	IP - Privacy	PET deployment	1		1	1	1	2	1
12	IP - Privacy	Redesign for PET	2		2	1	1	1	1
13	v6S - Ipv6	PKI deployment for IPv6 (Ike2)	2		1	1	1	2	2
14	v6S - Ipv6	Distributed end-2-end security models	1		1	1	1	2	1
15	v6S - Ipv6	New security vulnerabilities brought in by IPv6	1		1	2	1	2	1
16	SP - Policy	Security Analysis					1	2	
17	SP - Policy	High level policies				2	1		
18	SP - Policy	System Modelling			2		1		
19	SP - Policy	Security capability language				2	1		
20	WS - Wireless	Convergence				1	1		1
21	WS - Wireless	Security Roadmap			1	2	2		
22	WS - Wireless	Integration/harmonisation of exisiting and new technologies				1	2	2	
23	DT - Dep. & Trust	trustworthy adaptation to increased complexity	1		1	1	1	1	2
24	DT - Dep. & Trust	Balanced trustworthiness / security	2		1	2	1	1	2
25	DT - Dep. & Trust	Rethinking availability	2		1	2	1	1	2
26	MSC - Standards	Response time of standards development process			2	1			1
27	MSC - Standards	Shorten time of standards development process			2	1			1

Annex II – continued.

No.	Initiative	STF Challenge	Empowerment	EU specific needs	Availability	Interoperability	Development	Preservation	User-centric standards
28	MSC - Standards	Community participation in standards development						2	1
29	MSC - Standards	Certification				2	1	1	
30	SR - Research	Building in security from the start of the process	1			1	1	2	1
31	SR - Research	Privacy	1			1	2		1
32	SR - Research	Security in a heterogeneous environment	1		1	1	1		1
33	BS - Biometrics	European Biometrics leadership	2		2	1	2	2	2
34	BS - Biometrics	Promote European Values for identity in the network	1		2	2	2	1	1
35	BS - Biometrics	Leading Europe rowards cutting-edge Biometrics	1		2	1	1	2	2
36	CR - Crypto	Cryptography in an ambient ICT world	2		1		1		2
37	CR - Crypto	High performance cryptography			1		1		
38	CR - Crypto	Advanced Crypto for Media Protection			1		1	2	
39	SVP - Virt. Paradig.	Semantic co-operative standards	2			1	1		2
40	SVP - Virt. Paradig.	vitual communication domains management	2			1			
41	SVP - Virt. Paradig.	S&T Threat Assessment					1		
42	SVP - Virt. Paradig.	S&T Threat Pre-emption						1	
43	SVP - Virt. Paradig	Socially intelligent fixes	2					1	2
44	SVP - Virt. Paradig	Network Configuration security context sensing and Situation Assessment	2					1	
45	SVP-Vir. Paradig.	supporting delegated personal security and privacy protection management -proxy-enabled	1						2
46	SVP-Vir. Paradig.	Dynamic Grid Security: grid-aware live applications context-aware security SLA contracting	2				1		
	SVP-Vir. Paradig.	Network security and trust on the internet						1	
47	DAMI	Development of secure and robust watermarking algorithms				2	1		
48	DAMI	(watermarking) and non intrusive (digital forensics) techniques			2	2	1	1	
49	DAMI	Asset identification: perceptual hashing				1			
50	DAMI	Conditional access to the digital assets	1		2				
51	DAMI	Asset processing in the encrypted domain	1				1		
52	DAMI (& IPI)	Covert Communications (steganography and steganalysis)			2	1	1		