ICT Trust, Security and Dependability Research Strategy beyond 2010.

James CLARKE[1], William Donnelly[1], Zeta Dooly[1] , Michel Riguidel[2]
[1]*Waterford Institute of Technology, Cork Road, Waterford, Ireland*
Tel: +353719166628, Fax: + +35351302902, Email: jclarke@tssg.org
[2] *ECOLE NATIONALE SUPERIEURE DES TELECOMMUNICATIONS, 46 rue Barrault, Paris 13, 13, 75013, France*
Tel: +33(0)145817302, Fax: + 33(0)145813119, Email: riguidel@enst.fr

Abstract: This paper, entitled **ICT Trust, Security & Dependability Research strategy beyond 2010**, will describe the final outputs of the IST SecurIST [1] project, whose objective was to create a clear European level strategy to drive ICT Security and Dependability research beyond 2010. The focus in the paper is on short to medium (up to 3 years) to long-term objectives (~3-10 years). This paper will develop the context of the project, the approach taken, research strategy, setting its objectives and results with reference of various inputs and outputs from a large constituency involved in ICT Trust, Security and Dependability areas that was ultimately co-ordinated by the SecurIST project.

Keywords: Trust, Security, Dependability

1. Introduction

Trust, Security and Dependability (TSD) is a discipline that changes day by day, along with the wide deployment of digital (fixed, mobile, wired and wireless) technologies, and their penetration in all aspects of human activity. The advent of ubiquitous computing and communications that facilitate log on and the processing of data in network infrastructures anywhere/anytime, are the main causes of today's growing computer delinquency phenomena. Cyber-crime, the natural extension of real life violence in the virtual world, is compromising the intended handling and operation of digital information and systems.

The evolution of ICT security is governed on the one hand by technological progress (miniaturization of computers, progress in optics) and the consequent emerging vulnerabilities, and on the other hand by the growth in applications, the increased uptake of digital technology in all sectors of the economy and our daily lives and their consequent threats and malfunctions.

The demarcation between physical space and cyberspace will decline by the year 2010. The availability of abundant computing and networking resources, spread of critical data over these resources, and enhanced reliance of organisations and the general public on information technology will attract more attackers as their reward increases. To improve reliability of these edifices, new abstractions must be created in order to invent efficient paradigms; it is also necessary to design new TSD models, production tools using new programming languages, and protocols with modelling, simulation and verification techniques.

The goal of the fast expanding area of resilience 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 large public. In the short term, TSD research must obviously take into account the nature of technological progress and the constantly evolving demand and behaviour, but it must also set itself longer term objectives of a more general nature.

The following paper contains a description of the objectives and results of the SecurIST project in order to co-ordinate the bringing together of the TSD communities to highlight the appropriate and necessary strategy for the short, medium and long term areas of research and development that the EU must undertake in the 7th Framework programme.

1. Objectives

Our society is rapidly adopting more information and communication technologies (ICT) in services and commerce. Therefore, private information is at increasing risk and security and reliability problems become prevalent. Indeed, today people are becoming more and more concerned about the increasing complexity of information and communication systems and the proliferation of privacy-invasive information gathering sources and techniques. In their online daily interactions, they often find themselves faced with high-profile losses of their personal information and with viruses, spam, phishing and other crimes of growing severity and sophistication. As a result, they find themselves in an undesirable situation in which they must put ever more trust into environments in which there is little or no way of understanding or assessing them properly.

To build an information society that will deliver growth and prosperity, we need to tailor ICTs to business and social needs, and ensure that they become useful tools for economic and social innovation. The starting point for making them useful is to foster trust and safeguard security in a networked world. In this respect, Europe's research framework programmes are committed to the establishment of a solid security and dependability infrastructure. The IST-SecurIST project has been charged with the preparation of a European strategic research agenda in the field of ICT for Security and Dependability, for the upcoming 7th research framework programme (FP7, 2007–2013). In order to achieve this objective, the SecurIST project has established two fundamental bodies: the European Security and Dependability Task Force (STF), and the SecurIST Advisory Board.

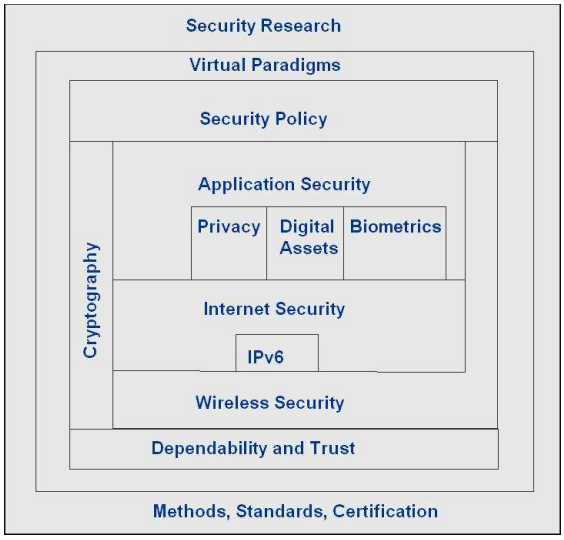

Figure 1. STF Intiatives integration

The STF is currently comprised of 200 members, spread across thirteen fundamental thematic areas (initiatives) of research. It provides a forum for consolidation and consensus building. The thematic initiatives are shown in figure 1, which provides a visual interpretation of how these initiatives are integrated and work together.

The SecurIST Advisory Board is composed of European experts in information security and dependability. The charter of the board is to oversee, review, enhance and promote results from the STF (see *www.securitytaskforce.eu*).

2. Methodology

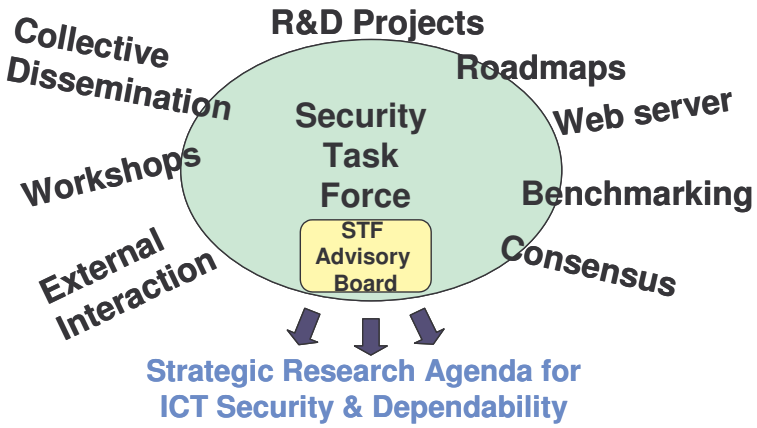

Figure 2. SecurIST approach

The approach and method taken by the SecurIST project in developing the Strategic Research Agenda for ICT Trust, Security and Dependability can be seen in Figure 2.

As mentioned, the project established two fundamental bodies – the EU Security and Dependability Task Force (STF) comprised of mainly members from former FP5 and FP6 projects and an Advisory Board (AB), whose interactions can best be described throughout the four project phases in Figure 3.

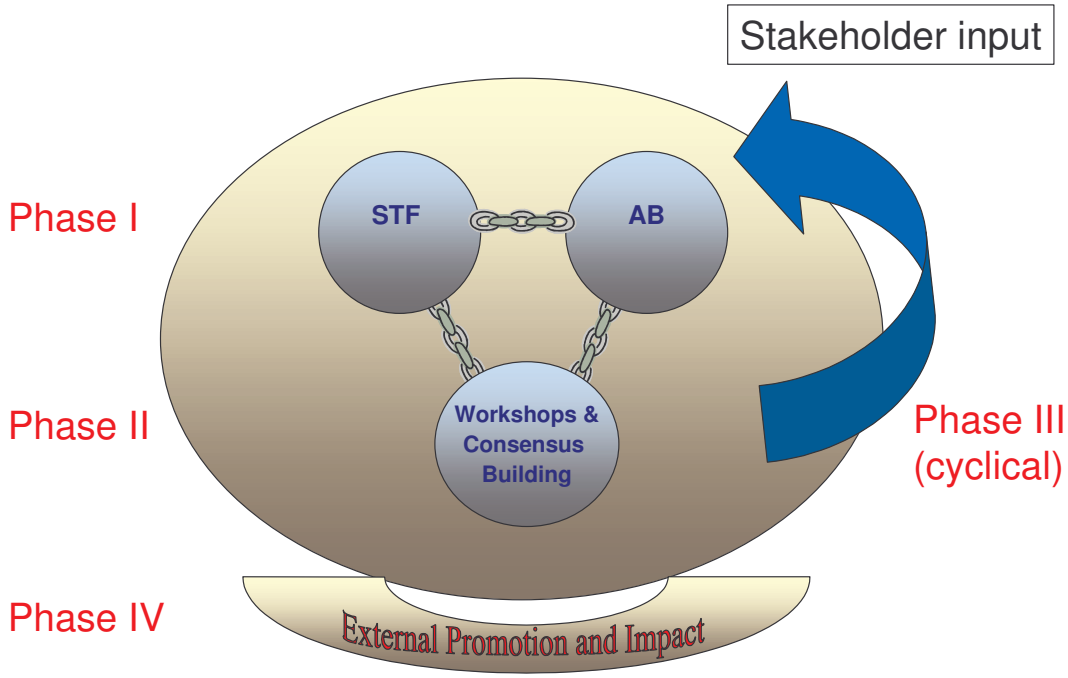

Figure 3. Interactions between STF and Advisory Board throughout SecurIST.

3. Overview of short and medium term challenges (2007 – 2010)

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. 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 fix or mobile. Their emergence will create new, unprecedented challenges for Trust, Security, and Dependability and Privacy.

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.

In the short to medium term, before 2010, research will mainly focus on:

- Cryptography: cryptographic mechanisms that require less resources, particularly in a constrained environment; cryptographic mechanisms for rights and assets management (DRM and DAM) guaranteeing their traceability; and flow encryption methods that are as safe, yet more effective, than current block encryption methods;
- Resilience, security and dependability of large critical infrastructures: The management of crises amplified by the domino effect; the protection of critical infrastructures and methods and tools for making them resilient;
- Ambient Intelligence security and virtual security: new security paradigms that meet the requirements of ubiquitous applications, establishment of trust without basing oneself on an existing infrastructure or organisation, low connectivity or intermittent connectivity structures, medium guarantee level as compared to the ordinary search for absolute assurance;
- Network security: fixed and wireless, mobile, active, ad hoc;
- Identification and authentication of players, contents, and rights management;
- Biometrics: large databases for the calibration and benchmarking of recognition algorithms, signature with biometrics, behaviour recognition by following a person and analyzing its gestures;
- Watermarking of images, sounds, video data flows, and software programs: protection of assigns, control of copies, authentication, integrity;
- Steganalysis: detection of hidden data using steganographic methods;
- IS security: techniques for intrusion detection, privacy protection, grid security, bait system architectures;
- Modelling and implementation of security policies: introduce the space and time, the context and the mobility, manage security policy conflicts, and model large infrastructures and security policies for health and medicine and for public administrations;
- The realistic assessment of vulnerabilities from the operational point of view, virus stopping, spam screening upstream from the end user's terminal;
- Certification, the assurance of security: introduction of incremental, faster and less costly, security assessment methodologies.

While considering the short to mid-term evolution of both technological and socio-economic aspects as presented above, the goal is to build on top of these 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. In this context, the next sections discuss the main research directions of work that have been identified for this (r)evolutionary period.

4. Overview of Long term vision of security challenges (2010 – 2020).

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 Trust, 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[1]. 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, 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 trust, security and dependability.
- 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 trust, security and dependability 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 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.

---

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

In the future, it will not just be individual computers that are targeted by hackers. One has to reckon with a rapid increase, for example, in attacks on name servers (Domain Name System or DNS), which are responsible for allocating host names to IP addresses. Attackers are increasingly focusing on routers, firewalls and other security tools, which are intended to protect the systems of companies and administrative bodies. Such attacks have a new detrimental quality since entire computer networks are affected by them.

The demarcation between physical space and cyberspace will fade away by the year 2010. The availability of abundant computing and networking resources, spread of critical data over these resources, and enhanced reliance of organisations and the general public on information technology will attract more attackers as their actions become more rewarding.

5. Results

The SecurIST project endeavored to include as many participants and projects within the STF Initiatives and held a special Workshop in March 2006 to fast track the inclusion of the Information Society Call 5 Security and Dependability projects within the Security and Dependability Task force membership. This was a crucial milestone as it enabled the incorporation of a number of other very important challenges not originally captured in the STF work to be included in the analysis by the SecurIST Advisory Board; For example, in the software and services areas, Service Oriented Architecture (SOA), were included in the subsequent output reports. In addition, SecurIST held a dedicated Workshop [2] in May 2006 bringing together the Mobile and Wireless and Security and Dependability Communities for the first time to intensively discuss and agree the mutually important challenges and issues for their constituencies. All of these challenges are detailed and contained in [3].

A large number of detailed challenges and priorities for FP7 were elicited from the EU Security and Dependability Task Force Initiatives and these were presented to the SecurIST Advisory Board for review both in writing and in presentations at Workshops. The challenges were aggregated and weighted into R&D focus areas by the Advisory Board with the assistance from the STF and discussed at a number of dedicated workshops. The Advisory Board then mapped these challenges to a higher level set of recommendations and clearly defined these recommendations in a very detailed recommendations report [4] for a future security and dependability research framework in Europe, for the period 2007-2013.

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[2], integrity and availability of information and seeks to

[2] including privacy aspects

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.

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. 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.

Under the headline *From "Security and Dependability by Central Command and Control" to "Security and Dependability by Empowerment"*, the Advisory Board is recommending the following nine key research areas:

1. **Empowerment of the Stakeholders:** Stakeholders of the information society include individual citizens, industry and academia, non-governmental organisations and governments. Empowerment of the stakeholder is vital as there is a clear technological trend towards decentralization of technology, as well as of its management and control. Responsibility, authority and control have to move more towards the end user.
2. ***Europe-specific*** **Security & Dependability:** Europe has a very specific heterogeneous culture and history and set of attitudes to trust and society that requires specific research profiling. Thus, 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, further research efforts are needed for the assurance of ICT network and service infrastructures. 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 future research focuses on the interoperability between security and dependability technologies and standards.
5. **Processes for developing Secure and Dependable systems:** Research on the systematic improvement of secure and dependable system development (including hardware and software) from their design phase, 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 standardisation:** Strengthen the structured involvement of end users and their respective representatives into relevant standardization activities involving security and dependability technologies.
8. **Security and dependability of Service Oriented Architectures (SOA):** The need to establish and maintain trust and manage policy regulations and service level agreements in an SOA context, together with commensurate advances in software engineering to deliver service expectations.
9. **Technologies for security:** Underlying all of these other research areas 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.

In addition to these nine key research areas, four future *grand challenges* (covering a 10-20 year vision) are presented by the Advisory Board. They illustrate possible longer-term possibilities and implications.

1. **Countering vulnerabilities and threats within digital urbanization**: This challenge addresses open problems that we will face in security and dependability from the expansion and globalization of digital convergence by 2010-2015.

2. **Duality between digital privacy and collective security: digital dignity and sovereignty:** This challenge deals with future privacy issues of all the stakeholders, whether citizens, groups, enterprises or states. It addresses the problem of how to override the "Big Brother" syndrome and "dark security", i.e., the future assurance of digital sovereignty and dignity for the various stakeholders.

3. **Objective and automated processes -** ***the Reinforcement of the Science and Technical Foundations of TSD*****:** This challenge addresses the problem of how to attain

a controllable and manageable world of complex digital artefacts by 2015 and how to inject regular, quantitative techniques and engineering to make the field truly scientific.

4. **Beyond the Horizon: a new convergence - *Going beyond the Digital Universe*:** This last challenge deals with the preparation of a new convergence at a horizon of 2020 and beyond, which is the bio-nano-info-quantum "galaxy" and the new security and dependability challenges that will emerge.

6. Conclusions

The SecurIST project has been successful in establishing two fundamental bodies, which have mobilised the Trust, Security and dependability communities to provide valuable input towards a TSD strategic research agenda for Europe.

This paper has provided the reader an overview of the final results of the SecurIST project, the methodology used, and the outputs from the EU Security and Dependability Task Force and Advisory Board, which will both continue after the official end of the project. The paper also provides pointer for more detailed information on the outputs of the project.

In the next Call for the IST programme in FP7, there is a special call for collaboration with International partners in non European countries including Africa. Therefore, it is the intention of the authors to begin this process with the delivery of this paper and presentation in IST Africa 2007.

References

[1] http://www.securitytaskforce.eu
[2] Workshop report available at http://www.securitytaskforce.eu
[3] SecurIST Deliverable, **D3.3 ICT Security & Dependability Research beyond 2010 Final strategy**, January 2007.
[4] Lechner, et. al. **Recommendations for a Security and Dependability Research Framework: *from Security and Dependability by Central Command and Control to Security and Dependability by Empowerment,*** June 2006.