

# SecurIST: Ensuring Secure, Dependable & Resilient European ICT Technologies to Empower the Citizen, Protect Critical Infrastructure & Provide Economic Growth

Zeta Dooly, Willam Fitzgerald, James Clarke  
Telecommunications Software and Systems Group  
Waterford Institute of Technology,  
Waterford,  
Ireland.  
{zdooly, wfitzgerald, jclarke}@tssg.org

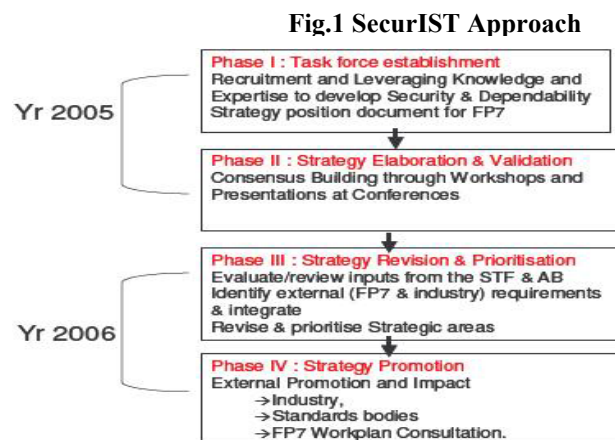
**Abstract**— To empower the citizen of the 21<sup>st</sup> century and Europe's economic prosperity over the next decade and beyond, Europe's Research Framework programmes are committed to the establishment of a solid security and dependability critical infrastructure. The IST-SecurIST FP6 project is charged with the coordination of a strategic agenda for ICT Security and Dependability R&D for the next framework programme of research and development in Europe (FP7: 2007 – 2013). The SecurIST project has established two fundamental bodies: a European Security and Dependability Task Force, (STF), drawn mainly from FP6 projects, whose role is to identify thematic Areas, and to identify and prioritise challenges within Security and Dependability research, and an Advisory Board (AB), comprising established experts, whose role is to review, advise, enhance and promote the STF and further prioritise areas for future research. This paper outlines the approach used, and gives preliminary results in achieving secure and dependable ICT citizen empowerment.

**Index Terms**— security, dependability, research, European 21<sup>st</sup> century security focus, citizen empowerment, economic prosperity.

## I. INTRODUCTION

Europe's Research Framework programmes (FP5-FP7) are committed to the establishment of a solid security and dependability infrastructure. The IST-SecurIST FP6 project, which commenced in November 2004 under the Strategic Objective *Towards a global dependability and security framework*, is charged with the coordination of a strategic research agenda for ICT Security and Dependability R&D for the next European framework programme (FP7: 2007 - 2013). This paper highlights the goal of SecurIST, strategic challenges and details the requirement to empower the citizen of the 21<sup>st</sup> century with real and usable security and dependability solutions.

The SecurIST research programme has four major phases (Fig. 1), whose aim is solving the following key objectives:



- Establish themed working groups to identify key challenges and priorities;
- Establish Advisory Board to assist in the direction and promotion of the research;
- Development of a security and dependability strategic research agenda and roadmap;
- Organise workshops involving experts from all Initiatives;
- Follow holistic approach to security to include new and existing technologies;
- Address Socio-technical challenges;
- Liaise with the European and National security agencies (ENISA), Institutional Advisory bodies (ESRAB) and so forth;
- Create awareness amongst all stakeholders and the users.

SecurIST is leveraging the expertise of existing projects and of the knowledge experts already engaged in ICT security & dependability R&D. For example, Table 1 shows all security related FP6 projects, which have been approached and categorized to highlight their research themes and main focus with respect to the STF thematic initiatives.

STF Initiative	WSI	IISI	ASI	DTI	BSI	IPI	CRI	SPI	SRI	MScI	SVPI
<b>Project</b>											
BIOSEC					**						
e-JUSTICE	**				*	*		*			
INSPIRED	**							*			
PRIME						**	*	*			
SECOQC							**				
SEINIT	**	*	*	*					*	*	
ECRYPT							**	*			
FIDIS						**		*			
BioSecure					**						
Digital Passport					**	*					*
MEDSI			**								
POSITIF								**			
SCARD							**				
SECURE JUSTICE		**			*	*	*	*			*
SECURE PHONE	*				**	*	*				
LOBSTER									**		
NOAH									**		
MOSQUITO	*	*	*	**				*		*	

Table 1<sup>1</sup>: Categorisation of FP6 Security projects into research Themes of SecurIST.

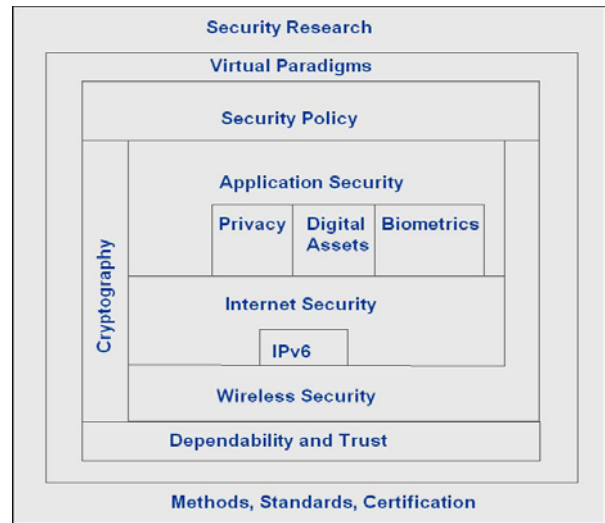
## II. SECURIST COMPOSITION

### A. Security & Dependability Taskforce

The Security & Dependability taskforce (STF) is currently comprised of 154 members, spread across thirteen fundamental thematic areas of research. There is a chair for each thematic area that co-ordinates the work within that thematic area and also liaises with the consortium. The thematic initiative areas of focus are:

<sup>1</sup> Table Key: double asterisk denotes the major field of security research and the single asterisk denotes sub-security research fields as a consequence of the major research field.

- Application Security -- ASI
- Internet Security Initiative -- IISI
- Identity & Privacy Initiative -- IPI
- IPv6 Security Initiative -- v6SI
- Security Policy Initiative -- SPI
- Wireless Security Initiative -- WSI
- Dependability & Trust Initiative -- DTI
- Methods, Standards and Certification Initiative MSCI
- Security Research Initiative -- SRI
- Biometrics Initiative -- BSI
- Cryptography Initiative -- CRI
- Virtual Paradigms Initiative -- SVPI
- Digital Assets / DRM Initiative -- DAMI



**Fig. 2: STF Initiatives**

Figure 2 provides a visual interpretation of how these initiatives integrate and co-operate with one another.

Each Initiative deals with a particular area of research in ICT security and dependability. For example, the ASI is directed at improved and novel approaches to application level security measures, new architectures and end-to-end security design issues to protect at an application level in future networks. The following areas of ASI are being investigated: security tools, policies, context management, allowing trusted users to view documents, single sign-on, digitally signing web pages, application vulnerability validation, anti-virus and so forth. The DTI is concerned with two main issues: the confluence between classical dependability and security, met essentially but not only by the concept of common 'accidental fault and malicious intrusion tolerance'; and the necessary but often forgotten link between trust (dependence or belief on some system's properties) and trustworthiness (the merit of that system to be trusted, the degree to which it meets those properties, or its dependability). For an in depth discussion on what each of the 13 initiatives cover, see [1], [2] & [3].

### ***B. Advisory Board***

The SecurIST Advisory Board is composed of European experts in information security and dependability. The Advisory Board has delivered several documents and given presentations on preliminary findings [3], [5], [6]. The Board has also established and will continue establishing links to other relevant European activities and bodies of significant relevance. For example, the European Security Research Advisory Board, ESRAB and the European Network and Information Security Agency, ENISA.

The SecurIST approach is from the Information Society's stakeholder's point of view and is, therefore, complementary to the approach of the European Security Research Advisory Board ESRAB<sup>2</sup>, 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<sup>3</sup>, which focuses from an ICT point of view on CERT co-operations, risk management and security awareness.

### III. CHALLENGES AND RECOMMENDATIONS

The STF is examining the challenges of a paradigm shift of gradually replacing the physical boundaries with logical boundaries maintaining context in order to move from a system-centric, or “Central Command and Control” to a Citizen centric, or “Empowerment of the Citizen” approach to security. Few ICT technologies have been designed with this kind of scenario in mind so a gradual process of revisiting basic technologies is required to ensure that the context sensitive empowerment of the citizen is supported. The transformation will be much more than a quick fix and will require a sustained effort on all levels to ensure understandable, interoperable, secure, convenient and efficient systems.

The SecurIST Advisory Board has aggregated, weighted and enhanced the results from the STF initiatives and has come to the conclusion that for a secure and dependable Information Society in Europe, the following seven technological and socio-technical areas need to be addressed in a European Security and Dependability Research Framework:

- ***Infrastructure availability:***

Assurance of ICT infrastructure robustness and availability

- ***Interoperability:***

Interoperability between security and dependability technologies and standards

- ***Secure and Dependable Development:***

Systematic improvement of secure and dependable system development right from the start

- ***Security and Dependability Preservation:***

Keeping up security and dependability in a more and more complex world

- ***End user centric security and dependability standardization:***

Strengthen the structured involvement of end users and citizens or the respective representatives or institutions into standardization activities around security and dependability technologies

<sup>2</sup> see European Commission's Regulation 2005/516 of April 22, 2005.

<sup>3</sup> <http://www.enisa.eu.int/>

- ***European Security and Dependability:***

In the research activities, specific European requirements have to be taken into account. Europe has a very specific heterogeneous set-up in culture, trust and history that requires specific research profiling.

- ***Empowerment of the Stakeholder:*** Empowerment of the stakeholder is highly important as there is a clear technological trend towards decentralization of technology, management and control.

The SecurIST Advisory Board is working on a Recommendations report [6], whereby the results of this report, further interim conclusions and recommendations from the project and the above workshop will be presented in the final version of this paper, and at the IST Mobile and Wireless Summit, allowing opportunity for further reflection and consultation to allow consideration, in mid-2006, of foresight of necessary directions for 2010 and beyond.

#### **IV. EMPOWERING THE CITIZEN**

The empowerment of the citizen requires a different paradigm of an approach to security and dependability than the traditional view and needs to stretch across individual perceptions of security such as trust relationships, user friendliness and granularity of security mechanisms, together with the dependability and reliability of those mechanisms. The citizen's perception of security and dependability is and will be heavily influenced by his/her awareness of the need for security and dependability and his/her trust or distrust in information society technology. Therefore, user-centric aspects should be the fundamental core elements of security and dependability, which is, of course, in conflict with the traditional industry or government-based control approach.

Shifting towards the new secure paradigm will involve addressing issues such as:

- Privacy is a high priority. Personal data is of utmost importance to the citizen;
- The ICT needs to regain the confidence of the citizen;
- Provide real systems and services solutions that have value and are useable by the citizen;
- Educating the citizen will be a key factor in promoting a secure and safer environment.
- European law must remain strong and in favour of its citizens right to privacy.

Empowerment of the citizen is currently limited if not impossible as there is no environment to apply the above measures. This is what SecurIST is striving to achieve in building a roadmap for future European research that will deliver the goals of citizen-based security and dependability.

#### **V. CONCLUSION**

This paper has highlighted the goal of SecurIST, identified challenges and the requirement to empower the citizen of the 21<sup>st</sup> century with real and usable security and dependability solutions. A considerable amount of effort has gone into the formation

of the Security Task Force initiatives and Advisory Board and the elaboration and consensus of the key challenges from the technology and the socio-technical perspective. However, it is abundantly clear that there is still considerable work to be done and it is the intention of this paper to introduce and generate real discussions and debate amongst the mobile and wireless communities whom will have a vital role to play in the shaping of the strategic research agenda for ICT Security and Dependability in Framework programme.

#### REFERENCES

- [1] Clarke, J. & Fitzgerald, W. , "SECURIST: Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D", in 39TH Annual IEEE International Carnahan Conference, 2005.
- [2] Clarke, James Fitzgerald M. William, "SecurIST: Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D ", Information Security Solutions Europe, ISSE, Budapest, Hungary, September 2005.
- [3] Security Taskforce Repository: <http://www.securitytaskforce.org/>
- [4] Fitzgerald M. William, Clark J. James, "SecurIST Inaugural Workshop Report" Brussels, 2005,  
<http://www.securitytaskforce.org/>
- [5] Clarke J. James, Fitzgerald M. William, "SecurIST Second Workshop Report" Brussels, 2005,  
<http://www.securitytaskforce.org/>
- [6] Lechner S., et. al. "SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework", March 2006.