



**SIXTH FRAMEWORK PROGRAMME
PRIORITY 2
Information Society Technologies**

COORDINATION ACTION



***SecurIST* Inaugural Workshop**

On

ICT Security & Dependability Research strategy

Date: 18th January 2005

Time: 09:30 – 17:30 CET

***Centre de conferences, Albert Borschette, ROOM AB-0A, rue Froissart,
36 B-1040, Brussels***

Project acronym: SecurIST

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

Proposal/Contract No.: 004547

Project Document Number: SecurIST/050118/M/v0.1

Project Document Date: 21/01/2005

Workpackage Contributing to the Project Document: WP1

Deliverable Type and Security: R¹-CO

Author(s): William Fitzgerald, Jim Clarke

¹Type: P - Prototype, R - Report, D - Demonstrator, O - Other



Table of Contents

Executive Summary	3
What is SecurIST?	4
Organizational Structure	4
Working methodology	5
SecurIST inaugural workshop minutes	7
Introduction to security taskforce opened by Dr. Willie Donnelly	7
European Strategic agenda on Security and Dependability by Jacques Bus, Head of the Security Research Unit in the European Commission's DG IST	7
Technical Keynote Presentations	8
Setting Security Priorities (2006-20010)	12
Overview and status of security research in Europe	13
Integrated Projects:	14
NoE Projects:	14
STREP Projects:.....	15
Additional Contributing Security Domain Presentations:	15
Forming the Task Force Working Groups	16



Executive Summary

There has been much discussion about the emergence of the knowledge society. The engine driving the creation of this society is an ICT framework based on the convergence of media, processes and communications networks delivering ubiquitous access to knowledge irrespective of location. Much of the ICT research agenda is focused on the specification of this framework. The proposed systems are highly complex requiring the interconnection of highly complex infrastructures and systems. The pervasiveness of ICT in this new society creates challenges in terms of privacy, access control, trust and reliability. The development of an effective secure and dependable environment is crucial for the effective delivery of the knowledge society.

The creation of a knowledge society within Europe requires that Europe position itself at the forefront of research in this area. The key challenges for Europe are to develop security solutions, which can guarantee dependability and resilience of ICT infrastructures and well as provide management and control capabilities for these networks.

The IST FP6 project SecurIST is addressing the challenge of developing a European Strategic Security Research Agenda for post FP6, designed to drive the development of the security research program for FP7. The project will act as a catalyst bringing together the key research scientists and industry decision makers to develop this agenda. Participation in the development of this agenda is open to all organisations interested in making a contribution to developing a European Security and dependability research agenda. The project has ensured uptake of its outputs by creating a security advisory board composed of key industrial experts and decision makers charged with providing guidance to the project in the development of the security research agenda and in promoting the projects outputs to industry.

This document provides a brief overview of the SecurIST and the minutes of its inaugural workshop on ICT security and dependability research strategy. Companies and projects wishing to join this initiative can register their interests at **www.securitytaskforce.org**.

We look forward to your participation.

Willie Donnelly, SecurIST project manager

What is SecurIST?

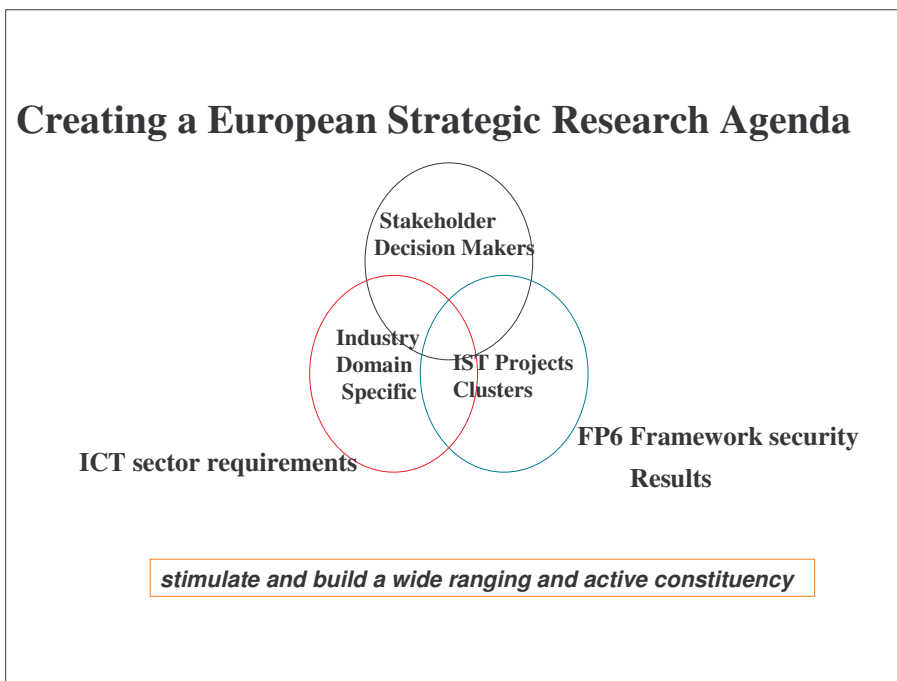
SecurIST is an FP project focused on the articulation and elaboration of a post FP6 European Strategic Research Agenda for ICT Security and Dependability R&D. This project will thus facilitate a smooth transition of the ICT security and dependability research agenda between FP6 and FP7.

The research agenda must

- ❑ Provide Europe with a clear European level view of the strategic opportunities, strengths, weaknesses, and threats in the area of Security and Dependability.
- ❑ Identify priorities for Europe, and mechanisms to effectively focus efforts on those priorities,
- ❑ Identify instruments for delivering on those priorities and a coherent time frame for delivery.

Organizational Structure

The project approach is to create consensus among the key European industry and academic players on the security and dependability research priorities for FP6. The approach is to build on what has already been achieved through the Framework 6 security workplan.





This is achieved through:

1. Creation of a security taskforce

The project will develop the FP7 research strategy in collaboration with the projects and people who are active in the security research programme in the present framework programme. The challenge is to bring the major players from the various ICT thematic domains to elaborate an integrated strategic research agenda which not only addresses their own area of concern but identified the challenges from the intersection of this area of interest.

The taskforce is creative engine charged with the development of the strategic research agenda. The security taskforce will be composed of industry and academic players involved in the IST security and dependability research activity particularly through the FP6 framework projects.

It is critical to prepare the groundwork for establishing a strategic research agenda for ICT Security and Dependability R&D through building on, aligning, and creating synergies between the different dimensions of security research. Through the use of clustering by thematic areas, the project will leverage the knowledge base of projects and people already engaged in Security & Dependability R&D. The thematic area approach will enable projects already engaged in aspects of Security & Dependability R&D to address how their research activity will contribute to higher level issues, and to the elaboration of the research Agenda.

Therefore, membership of the taskforce is open to all players and organisations actively involved in European security research. Registration is carried out through the website www.securitytaskforce.org.

2. Establishment and management of the Security Advisory Board

One of the main tasks for the project is the establishment of a security task force. At the heart of the task force is the Security Advisory Board. The Security Advisory Board will be composed of leading players in business (CEO,CTO level) and Leading players in the standards bodies (IETF, US Security task force). The role of the members will be to drive the SecurIST developed security strategy within the industry and funding organisations. Members must be recognised as key leaders in the technology fields, which we require to make an impact (such as wireless, 3G, internet, e-business).

Working methodology

Security taskforce working groups

The security task force will organise itself into working groups charged with developing the technical details which will form the basis of the security white papers and roadmaps. While the working groups will initially be structures around security research themes, the work of these groups will also address the interface between and dependencies across themes.



Key objectives for the working groups will include:

- *Benchmarking IST security results against evolving industry needs, by compiling results already available from IST and other related initiatives in Europe*
- *Defining security synergies/dependencies across industry and research sectors*
- *Exploring use cases and implementation strategies as example solutions*
- *Development of strategic security roadmaps.*

Themed workshops

The project will conduct a number of themed workshops designed to build consensus among the security and dependability research and development community.

The workshops will allow the projects and people already engaged in Security & Dependability R&D to actively contribute to the development of the research strategy by identifying the specific challenges resulting from the outputs from their own work and extrapolating their experience to address the more global research challenges for the future and emerging ICT systems.

The first step towards the development of the research agenda will be the production of a strategic white paper detailing the ICT Security & Dependability Research beyond 2010 Initial strategy. This white paper will support the promotion of research priorities with the IST programme as it evolves towards the 7th framework.

The themed workshops will:

- *Provide an environment for the IST security community to define the medium term (3-5) and long term (5-10) security research strategy*
- *Enable the external ICT community to contribute to the development of this research strategy*
- *Create consensus on priorities for Europe in ICT Security and Dependability research and provide an initial research strategy roadmap for framework 7 work programme*
- *Provide a platform to promote the prioritisation of ICT security and dependability research agenda in the emerging European Strategic Research Agenda (SRA).*



SecurIST inaugural workshop minutes

Introduction to security taskforce opened by Dr. Willie Donnelly

Dr. Donnelly described the current research as focused primarily on organizations and the individual activities of the consortia involved and how there are not enough coordinated activities in the boundaries of the specific areas within Security and Dependability. Thus, the Security taskforce aims to resolve this with a more coordinated and holistic approach to deliver a global solution. He states we aim to correlate these activities with two approaches:

1. **Top down approach:** task force looking at the various issues to give guidance to the projects;
2. **Bottom up approach:** ensure we are making good use of the positive work from within the projects. It is the intention to capture requirements and solutions from projects and feed into the roadmap.

European Strategic agenda on Security and Dependability by Jacques Bus, Head of the Security Research Unit in the European Commission's DG IST

Mr. Bus thanked everyone for attending and states that the Workshop is an excellent opportunity to build a co-ordinated platform to bring together the IST projects within this area. Mr. Bus hopes that the security Taskforce will play a vital role in bringing together the projects working in this area, thereby guiding the FP7 strategy process and possibilities for research agenda for the coming years.

Mr. Bus described the timings of the process within the European Commission and the Council decisions. Mr. Bus said that the first step was to present ideas for FP7 and these were discussed and accepted by the Council in September 2004. The work was supported by the Member states.

It is envisaged that the next step will take place in April of 2005, when the Commission will adopt the first draft for the FP7 Programme. Mr. Bus stated that SecurIST has a major role here. Mr. Bus pointed out that one of the lines that was accepted in the September 2004 decision was that there would be an EU Security Programme within FP7.

Mr. Bus said that security would be viewed in the sense of how the normal citizen thinks about their security. Hence, we will need to derive solutions with respect to demands and what is needed to fulfill the demands. One of these is, of course, relating to the ICT area. The ICT area will be further developed and will be more focused and critical infrastructure will be included.

Mr. Bus said that a draft version of the FP7 Programme will be ready in February 2005 in preparation for the submission to the Commission in April 2005.



Mr. Bus said that within the IST programme, real technology research will be taken up, for example, with resilience and dependence of systems, identity and privacy management, trust (in the internet), amongst others. Mr. Bus stated that it would be important to have the support of the projects in these areas towards identifying the crucial areas to be addressed in FP7.

Mr. Bus said that the next step in the process is the development of a stable work programme. Once stable, a first draft of the work programme will be put on the table. There are clear roles for recommendations and roadmap ideas that can be taken up for the development of this work plan.

Mr. Bus said that SecurIST should assist in building up a strong consensus amongst the areas and play an important advisory role to fill in these various policy documents and the strategies needed that we want to achieve. In order to succeed, it is very important to keep a broad perspective. Security is very important and should be covered by more than one unit.

Mr. Bus pointed out that it is vitally important to create real cooperation based on the various perspectives and bring the communities together that, up to now, have not worked together. For example, embedded systems with Mobile communities should be brought together. Mr. Bus stated that when these communities can be brought together in a coordinated fashion, SecurIST can play a strong role in making a significantly more secure ICT environment in Europe.

Mr. Bus concluded by stating that we need to keep an open mind to enhance creative thinking across borders and receiving the people from the various communities and as a result, we will have a positive result.

Technical Keynote Presentations

Research Challenges in Cryptology & Security by Prof. Bart Preneel, Universiteit, Leuven, Belgium

Prof. Preneel stated that cryptography is everywhere in today's society. He described the progression of cryptography in the 80's, 90's and to the present day. There are inherent weaknesses in the cryptography applications and at a lower level. He states that we should focus on hard research problems and not easy quick fixes. There have been reasonable Key establishment protocols since the 1990's and secure implementations in the latter years of the 1990's. The upgrade from weak cryptographic solutions has been very slow and needs to be addressed. He states DES is outdated and more work should be focused on AES. Quantum computing will make all current cryptographic protocols insecure. There are many challenges ahead such as understanding security of AES, Hash functions, Stream ciphers, Public key cryptology, resisting quantum computers, improvement of provable security, Ultra low cost crypto and Cryptology for long-term security.

Deploying an On Demand Vulnerability Management Infrastructure by Adrian Ionel, EMEA VP and GM Manager, Qualys Ltd.



Mr. Ionel states that understanding the prevalence of critical vulnerabilities over time in the real world is very important. He discussed how even with patches for vulnerable machines, machines are not being updated and so are still vulnerable to older attacks. He discusses the concept of “half life”. From analyses with their customers, the half-life of critical vulnerabilities is 21 days on external systems and 62 days on internal systems, and doubles with lowering degrees of severity.

50% of the most prevalent and critical vulnerabilities are replaced by new vulnerabilities on an annual basis. The persistence of the lifespan of some vulnerabilities and worms is unlimited.

He also stated that the vulnerability-to-exploit cycle is shrinking faster than the remediation cycle. So 80% of worms and automated exploits are targeting the first two half-life periods of critical vulnerabilities.

Their studies have found that significant progress has been made on the remediation cycle (30-to 21 days) for external vulnerabilities. Mr. Ionel stated that the end goal is the shortening of half-life of internal vulnerabilities from 62 days to 40 days within one year.

Mr. Ionel was asked this question “isn’t it very difficult for companies to do this on their own?”

Answer – Yes. For example, one of their customers, a well known large company, carried out an in-depth analysis of the vulnerabilities within their systems. They found that their systems had 100,000 vulnerabilities with 20,000 of these would be classified as Critical. Therefore, the order of magnitude is tremendous - it becomes a very daunting task and for most of these people have not had security as their primary priority. They have, for example, other priorities like system availability.

Identity Management in Mobile Communication Systems & their Applications by Prof. DR. Kai Rannenberg, University of Frankfurt, Germany.

Prof. Rannenberg described current identity management systems such as the Microsoft passport (>200 million users) and the liberty alliance (150 members). Prof. Rannenberg also discussed related approaches such as Trusted platform modules and eBay’s approach.

Prof. Rannenberg focused on SIM (Subscriber Identity Module) and describes uses for this technology, for example, SIM hardware as a platform, SIM info as a credential and GSM subscriber information as a profile.

Banks and mobile operators have put several authentication tokens on one SIM. He states that different domains are now working together on a one token device.

Prof. Rannenberg states that using SIM information as a credential would mean thieves would now need to steal your mobile phone and PIN number. GSM subscriber information being used as a profile could be used with mobile portals as an access concept for mobile devices.



The use of SIM's in society is also discussed and Prof. Rannenberg states that policy questions about data availability has to be researched.

The IT industry can put more high tech data on ID cards each and every day such as biometrics to bind them closer to a human being.

Prof. Rannenberg details challenges and potential for FP7. Examples include:

- user policy driven (determined) and privacy friendly access control,
- graceful integration,
- a secure identity carrier beyond the chip card or SIM: TPM phones or PDAs,
- careful evaluation of biometric patterns and mechanisms.

Prof. Rannenberg concludes by saying SIMS are a widespread global ID infrastructure. Application areas can grow beyond the standard mobile communication domain. Identity management is happening (silently).

Question: can this be extended to other areas e.g. automobiles?

Answer, Yes. For example, there is already an application in which the lead sheep has an embedded SIM for location logistics.

There was a comment from the floor that Identity management implies identity ownership. There has been very little done with regard to identity revocation whereby someone can revoke identity if it is being misused. There are also sub-levels of revocation. There is no research solution at the moment and there is a significant amount of information integrity management issues that need to be solved.

Significance of Dependable Infrastructure to Secure the Information Society by Prof. Paulo Verissimo, FCUL, Portugal ICT-Security

Prof. Verissimo discusses the attack, vulnerability and intrusion (AVI) sequence in detail.

He asks is there a common denominator in the way we address these problems.

Prof. Verissimo points out that there are more and more systems relying on open networks environment, Internet, COTS components, unskilled users, etc. It is envisaged that explosive growth of inconspicuous devices, forming the active environments of the ambient intelligence world. These devices may fail because they are attacked.

Some of the main problems:

- Applications that are critical (SCADA) supported by semi - open geographically dispersed infrastructure;
- Applications that are commercial, ie. B2B, B2C, were supported by very open extra power site based server compounds;
- Applications of mixed nature with regard to purpose, but whose distinguishing feature is being supported by ad-hoc collections of wireless and mobile entities, immersed in active environments of ubiquitous and inconspicuous devices.



Prof. Verissimo discussed opportunities that present themselves are:

- Reconcile uncertainty with predictability;
- Manage apriori undefined or evolving failure modes and system configurations;
- Manage exposure, interdependence, interference;
- Handle operation mistakes, unskilled users;
- Adapt to fault/attack ranges: from script kids to cyber terrorists; low to high-power attackers; benign to harsh environments;

Prof. Verissimo describes some research avenues such as Reference Models / Architectural frameworks for enabling Resilience and Generic Architectures for Dependable/Trustworthy/Resilient Systems.

Question: Dr. Donnelly asked how do the researchers integrate with the software community.

Answer: Selling upgrades is an excellent business model. Security has put this software dependability issue into the forefront. When attacks became more frequent, there was a great push for the software developers to improve their systems. We will see the effect of this eventually. From the research perspective, there should be a take-up of results. In terms of research, we are pointing towards forward looking approaches at problems.

Challenges for Applied Research by Mr. Paul Friessem, Fraunhofer Institute

Mr. Friessem describes the challenges for applied research.

The increase in machine-to-machine (M2M) needs to be addressed:

- Trustworthy, secure cooperation without possibilities for human interaction (ie. privacy problems);
- Construction of trust relationships beyond PKI;
- Integrity ;
- Secure and efficient administration of lots of digital identities is required;
- Easy to use concepts, usability is a major concern to avoid errors in the first place;
- Combine well know usage habits with security technologies e.g. use handwritten signatures.

He also discusses technology trends in Ubiquitous networks (anybody, anytime, anywhere, anyhow). They are consisting of heterogeneous networks, fix networks, wireless, mobile etc.

These systems need seamless secure service roaming, context aware services. There must be an undeniable evidence of resource usage (accounting, billing) and a guaranteed quality of security.

There must be a convergence of infrastructure and systems to achieve a cross enterprise electronic business processes, a synergy effect, and a work flow optimizations; e.g. remote control and monitoring of IT systems.



Mr. Friessem states there will be a growing number of attacks (automatic tools, remote attacks) so development of tools for automatic system surveillance including early warning is a good idea.

Mr. Friessem said the rise of software attacks (malicious code) give rise to the development of new analyzing methods, e.g. source code analysis, and we need methods of security engineering as a refinement of software processes.

Mr. Friessem points out some challenges ahead. The defined borders will disappear and, hence, blurring of internal and external systems. Relinquishment of perimeter protection (e.g. firewalls) in favour of integrated system security and staged control domains! Dynamic change of context and environment will mean context aware policies are needed, which require concepts for trustworthy mobility management especially personal mobility.

Mr. Friessem summarised as follows: there will be change of security paradigms necessary from perimeter protection to the holistic integrated system security, from central access controls to decentralized usage control, from patch management on demand to long term sustainable security, from security as a product to security as a dynamic process.

Setting Security Priorities (2006-20010)

Dr. Sathya Rao provided a brief overview of the current Framework 6 security related projects. The scope of the security and dependability projects covers a broad range of technical domains including the following:

- Physical Infrastructure
- Biometrics
- Cryptography (quantum, RSA, IDEA,...)
- Privacy and identity management
- Security policy, Standards and certification
- Socio-economic impacts

This work provides a good starting point defining a European Security roadmap, which will form the basis for the definition of the strategic research agenda. Dr. Rao re-iterated the SecurIST two prong approach to the definition of this research agenda namely;

- Top-down strategic research agenda for Europe for “Security & Dependability”.
- Bottom-up aggregation of technical achievements of the Framework Programme.

The outputs from the FP6 projects will contribute to the bottom up aggregation. The challenge is to build on this work and, in particular, to define the interdependencies between these technical domains.

Dr. Rao also presented an initial set of working groups

- Dependability and Trust Initiative
- Wireless Security Initiative



- Internet Infrastructure Security Initiative
- Applications security Initiative
- Security Research Initiative
- Security Policy Initiative

Additional working groups may be championed by the members of the task force.

Overview and status of security research in Europe

Mr. Keith Howker of Vodafone further developed the theme of security research in Europe. He proposed that one needs to establish an inventory for the FP6 security and dependability research programme with a particular emphasis on:

- Voids
- Overlaps
- Synergies
- and complementary purposes.

The development of a successful strategic research agenda requires buy-in from the key European industry and academic stakeholders.

The challenge for the task force is to define an initial set of key security and dependability research priorities by April 2005 to drive security and dependability requirements for next framework, FP7. The challenge is not to confine ourselves to what is happening in FP6 but to expand the scope beyond what is required today.

In order to achieve this, we need to ask the question “why Europe should do something in this domain”. We need to establish *what* are the key drivers that should convince the industry to invest in the proposed research agenda.

This was followed by FP6 Security and Dependability presentations.



Summary of the FP6 project presentations

Integrated Projects:

SEINIT by Andre Cotton, Head of TAI laboratory, Thales.

- Map user requirements to security system requirements;
- Transparency on privacy issue involved in security;
- Provide the feedback to the user;
- Ambient intelligence based security;
- Building of Trust – merging several ranking and integration of security Mechanism ;
- Security adapted to the current threats.

DAIDALOS by Yannis Katsaros, Lancaster University.

- Security with mobility:
 - secure neighbour discovery,
 - MIPv6 and AAA integration,
 - interdomain issues,
 - Key management.
- Security in sensor networks;
- Rule based support of pervasive use of private protection.

EJUTICE by Patrice Emmanuel Schmitz, Senior Consultant, Unisys Belgium.

- Secure Justice communication: Authentication by biometrics.

BioSec: Orestes Sanchez-Benavente, Telefonica I+D

- Leverage security across biometric authentication chain;
- Data protection, privacy security perception, usability, Acceptance, convenience;
- User centered issues (Legal framework);
- Technical (Multimodal biometrics);
- Certification;
- Applications;
- ROI and cost estimation.

NoE Projects:

Ecrypt by Prof. Bart Preneel, Universiteit Leuven, Belgium.

- Symantic techniques, asymmetric, protocols, secure and efficient implementations, watermarking and perceptual hashing ;
- Document on recommendations.

PRIME and FIDIS by Dr. Kai Rannenber, Goethe University Frankfurt.

- Biometric binding;
- Chips to add PKI;
- interoperability of IDs and ID management systems;
- Database of Identity management;
- PRIME: privacy and identity management – safe and secure transaction with privacy;



- User focussed identify management;
- FP7: user policy driven and privacy friendly access control, graceful integration ;
- Multilateral security: Security and protection.

STREP Projects:

POSITIF by Dr. Antonio Lioy, Politecnico di Torino.

- Policy framework: suitability, measurement, configurations, monitoring.
- Need of tools for security system development: policy languages, system description.

SecurE-Justice by Dr. Bruno Crispo, Vrije Universiteit of Amsterdam.

- Protection and security to communication and collaboration ;
- User ID management and content protection ;
- Security guidelines, Adapt the system to the user ;
- Easy to use (user interface) and management systems.

Digital Passport: Alfred Gottwald, Siemens.

- Security analysis of legislative framework;
- Process analysis;
- Mapping to ICAO framework;
- Security concepts.

Additional Contributing Security Domain Presentations:

Euro6IX by Jordi Palet, CEO/CTO, IPv6 R&D, Consulintel, S.L.

- How IPv6 deployment affect the security of a network ;
- Network based security: threats from outside (?): Centralized model, fault prone, not end to end ;
- Alternate: Host based security: centralised policy distributed to PEPs: Threats from anywhere, complex.

GST by Antonio Kung, Founder and Chief Technology Officer, Trialog

- Open market for telematics ;
- Multi-layer, transversal architecture, Trusted components.

TEHA: European application home alliance by Antonio Kung, Founder and Chief Technology Officer, Trialog

- Interworking across: multimedia, household appliances ;
- End to end layered security architecture ;
- Multi-network, policy based.

Commercial Requirements Secure Information Systems: Alan Stanley

- The need for security in information systems;
- Business impact;
- Compliance and Measurement Quality;
- Best practices;
- Provide low cost quality security system needed;
- Secure code development.

Forming the Task Force Working Groups

The final part of the workshops addressed the establishment of technical working groups charged with the task of development of a European security roadmap as a first step towards the specification of the Strategic Research Agenda. It was agreed that the following terms of reference would define the operation of the groups.

- ❑ Any initial set of working groups will be established based on the key security research areas identified in the workshop
- ❑ Any member of the security task force could propose the creation of new working groups provided it added value to the work of the established working groups.
- ❑ The working groups will collectively contribute to the development of the technology roadmap.
- ❑ The working groups will align their work to ensure that they address areas of synergy and interdependencies between them and thus ensure that the project produces an integrated ICT security framework as opposed to individual technology or theme specific solutions.
- ❑ A number of themed workshops would provide a platform for consensus building across the work groups.

The Security task force initiatives identified so far:

- Wireless Security Initiative (WSI) - co-chairs: Bosco Fernandes – Siemens and Keith Howker – Vodafone.
 - Emails: Bosco Fernandes <bosco.fernandes@siemens.com> and Keith Howker <keith.howker@vodafone.com>
- Internet Infra Security Initiative (IISI): Chair: Miguel Ponce de Leon
 - Email: Miguel Ponce de Leon <miguelpdl@tssg.org>
- Apps Security Initiative (ASI) - Chair: Jim Clarke.
 - Email Jim Clarke <jclarke@tssg.org>
- Dependability & Trust Initiative (DTI) – Chair: Prof. Paulo Verissimo.
 - Email: Prof. Paulo Verissimo <pjv@di.fc.ul.pt>
- Security Research Initiative (SRI) - Chair: Sathya Rao.
 - Email: Sathya Rao <Rao@telscom.ch>
- Policy Consensus Initiative (PCI) - Chair: Antonio Lioy.
 - Email: Antonio Lioy <lioy@polito.it>
- New Initiatives proposed since January 2005 Workshop:



- Biometrics Security Initiative² (BSI) : Proposed Chair: Orestes Sanchez-Benavente.
 - Email: Orestes Sanchez-Benavente <orestes@tid.es>
 - Smart Cards Initiative³ (SC): Chair To Be Recruited (TBR)
 - Digital Asset Management Initiative (DRMI): Chair TBR
 - Cryptography Research Initiative (CRI): Chair TBR
 - Security Architecture and virtual Paradigms Initiative (SVPI): Chair TBR
 - Identity Management Initiative (IMI): Proposed Chair: Kai Rannenberg.
 - Email: Kai Rannenberg < Kai.Rannenberg@m-lehrstuhl.de>
-
- Please use the SecurIST website www.securitytaskforce.org to register as a member of the SecurIST working groups.
 - We would also request that you email the Chairs directly when registering to introduce yourselves and please cc. to Rita Dalton <rdalton@wit.ie>.
 - If you would like to propose yourself as a Chair (or Co-Chair of any of the above initiatives, please email your request to Rita Dalton rdalton@wit.ie at your earliest convenience as it will be on a first come, first served basis.
 - ***Date of next meeting : April 19th Brussels***

² Biometrics Security Initiative (BSI) interested in new algorithms, alternative solutions, novel pattern recognition approaches, multi-modal biometrics, data fusion issues, standardization of testing bio data and so forth.

³ Smart Cards Initiative (SCI) Mainly concerned with cryptography design, authentication, digital signature, protocols, contact-less, security standardization and international co-operation.