# Strategic Research Agenda for Security and Dependability in R&D

James J. Clarke, William M. Fitzgerald,
[1]*Waterford Institute of Technology, Telecommunications Software and Systems Group (TSSG), Cork Road, Waterford, Ireland*
*{jclarke | wfitzgerald}@tssg.org*

## Abstract

Industry and companies are benefiting significantly from the increased productivity, competitiveness and customer satisfaction provided by mobility. However, to be viable in the future, mobility must address the foremost challenge confronting it today ensuring a high level of security to protect the enterprise network and the valuable information it carries, dependability along with subscriber privacy issues. With the advent of mobility, security is even more important than before. Any existing vulnerabilities of the wired network can be opened to attack if wireless access is not secure.

The SecurIST initiative is a European consortium whose goal is to coordinate and consolidate the open challenges in Security and Dependability. The main objective of the SecurIST project is to deliver a Strategic Research Agenda for ICT Security and Dependability R&D for Europe. It will do this through meeting the following objectives:

- Establish and co-ordinate a European ICT Security & Dependability Taskforce (referred herein as Security Taskforce);
- Drive the creation of an "ICT Security & Dependability Research strategy beyond 2010";
- Leverage the knowledge base of existing/future ICT Security and Dependability researchers and projects.

After a short abstract (no more than 200 words) your paper should introduce your topic, explain your goals and make clear why your paper is distinct from similar works. Following a description of your results, finish with your conclusions and/or an outlook. The last section “Literatur” should contain a bibliography of works referred to in your paper. Your paper should be between 8 and 12 pages in total.

# 1 Introduction

The Strategic Research Agenda to be developed by the Security Taskforce will elaborate the ICT Security & Dependability Research strategy beyond 2010. It will provide a clear European level view of the strategic opportunities, strengths, weaknesses, and threats in the area of Security and Dependability. It will identify priorities for Europe, and mechanisms to effectively focus efforts on those priorities, identifying instruments for delivering on those priorities and a coherent time frame for delivery.

Through the use of clustering highly relevant thematic areas, the project will leverage the knowledge base of projects and people already engaged in Security & Dependability R&D. The thematic areas will enable projects to address how their research activity will contribute to higher-level and broader perspective issues, and to the clear elaboration of the Strategic Research Agenda.

The first step is the establishment of a credible European ICT Security & Dependability Taskforce. This taskforce will be constituted and coordinated through the SecurIST project, which will act as the Secretariat and Steering committee of the Taskforce. A core taskforce of 20-25 key players/influencers is complemented by a wider taskforce of 200-400 providing the basis for the structured emergence of a 'European Technology Platform' in ICT Security and Dependability in FP7.

This paper's central core will be structured around three areas of our findings:

1. **Categorisation of future Security Research:** where we define and develop research categorisations for future research and development.
2. **Analysis of ongoing Research Activities:** here we depict current FP6 security research trends based on our results of **Categorisation of future Security Research.**
3. **Themed Workshops Outcomes**: This section presents a short summary of the major challenges ahead as set out by the key speakers who presented their research at the workshops in January 2005 and April 2005.

## 1.1 Categorisation of future security research

By categorising security research into definitive areas as described below, one can readily choose an area of research to focus on and then define what needs to be addressed in that space. The following areas of security and dependability research today have been identified and the following Initiatives were established since the Inaugural Workshop held in January 2005 under the umbrella of the Security and Dependability Task Force (STF).

**Dependability and Trust Initiative (DTI)**

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).

**Security Policy Initiative (SPI)**

The ICT systems have become so complex that it is nearly impossible to design and manage their security in a global and reliable way. We envision to use a formal policy as the foundation to create computer-assisted security design and management system to support managers in the difficult task of defining and implementing a desired protection policy. Given an adequately high and general level of the policy, this should let managers concentrate on high-level rules rather than implementation details (that could be automatically derived by appropriate tools). Moreover an high-level policy would be also beneficial for auditors by providing them with a formal specification to check compliance with user requirements and measure actual achievements.

**Wireless Security Initiative (WSI)**

This initiative targets security in Mobile/ Wireless service environments. It will address Ambient Radio, Ambient Networks and User Device capabilities in a 3G/3G beyond, Ad-hoc and All IP networks. It will address mobile, wireless and smart card technologies covering the development of new protocols, interfaces, technology interoperability and future standardisation issues in this space.

**Security Research Initiative (SRI)**

Security Research Initiative (SRI) is an initiative for linking results of different research groups and initiative into one cohesive vision for the European research and development strategy addressing security and privacy in ICT. The terms of reference of SRI includes:

- Innovative network security architecture and models, including
  - new cryptographic paradigms and novel multi-party cryptographic protocols that can be easily adapted to different security policies and that can enhance the configuration of policies.
  - new approaches to defining security policies not necessarily based on access control, which may not be a viable solution in a mobile environment.
- New protocols for identification and authentication of nodes, services, routes, active code, etc. as well as for distribution of credentials
- Coping with new attack models such as distributed denial of service attacks
- Multi-party security association management
- Issues related to management of sources of trust and accountability in dynamic environments.
- Survivability of infrastructures, including assurance of unbounded and novel network types (e.g. “mobile” networks)
- Common security framework for both wireless and wireline architectures
  - Providing uniform access to security functions from a user’s perspective.
  - Rethinking the access control function to subdomains, when dealing with increasing number of domains and increased heterogeneity and to the user (personal) sphere.
- The importance of security standards to avoid proliferation of interworking and interoperability procedures.

**Application Security Initiative (ASI)**

This initiative 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 are being investigated: security tools, policies, context management, allowing trusted users to view documents, single sign-on, digitally signing web pages for example, application vulnerability validation, anti-virus and so forth.

**Internet Infrastructure Security Initiative (IISI)**

Focuses on security models and technologies for GRID, advanced cryptography for multimedia Internet and e-commerce applications, secure software for the future Internet, novel trust and security models for Internet and interoperable ubiquitous computing environment, de-

pendable home connectivity as the advent of ambient intelligence, privacy, authentication, accounting and reliability for Internet.

**Identity & Privacy Initiative (IPI)**

This initiative addresses research focusing on digital identity management, privacy protection and mediation, personal data environments and the development and use of privacy-enhancing technologies, (self-)management of privacy, as well as privacy and authentication mechanisms within fixed and mobile/wireless network environments.

**Biometrics Security Initiative (BSI)**

The initiative is interested in the elements dealing with the integration of biometrics in ICT systems, enabling new technology development in basic biometric technologies to leverage trust, confidence and security, across biometric authentication chain and identifying key features to put the technology to work and to meet requirements of real world applications. Interest also includes: new algorithms, alternative solutions, novel pattern recognition approaches, multi-modal biometrics, data fusion issues, standardization of testing bio data and so forth.

**Security Architecture and Virtual Paradigms Initiative (SVPI)**

Exploring socially intelligent architectures for best value ubiquitous management of the dynamic Security & Trust (S&T) chain across time, place and space; end-to-end. This research area involves architecting the semantic representation of distinct communicating domains and their enclosures (boundaries, sub-systems) so as to facilitate S&T services selection, composition and in general dynamic context-dependent S&T matchmaking for adequate security protection of each interacting domain and entity. This entails providing adaptive and personalised protection for each entity through distributed management and delegation of security protection to smart grid-enabled proxy services. Such security services should be invocable ubiquitously when required on a Call-by-Call security services outsourcing basis.

**Methods Standards Certification Initiative (MScI)**

The MSc Initiative of the Security Task Force is placed clearly within the existing European Commission policy on security with reference to

- Interoperability of security
- awareness building on existing security standards and their promotion
- the evolution of present security standards
- development of new security standards where appropriate
- Facilitating the existing security standards development process via
  - National Standards Bodies & International Standards Organisation
  - European actions through CEN/ISSS, CENELEC, ETSI
- Involving the New member States and User organisations in the Security Standards development process
- the existing framework of policy making, strategy and the structuring of the standards world. (European parliament, European Commission, ENISA, ICTSB (NISSG), and all the standards organisations).

**Cryptology Initiative (CRI)**

Focusing on advanced and novel cryptographic algorithms and protocols and techniques for watermarking and perceptual hashing techniques. The goals are to improve security and confidence in these techniques, to develop secure and efficient implementations and to integrate these techniques into advanced applications such as electronic voting, fighting spam, digital asset management and privacy enhancing technologies.

**Digital Asset Management Initiative (DAMI)**

Developing novel watermarking and stereophony algorithms, advanced cryptography, standardization of services for digital rights management and payments, securing CD/DVD copyrights, virtual electronic licensing and so forth.

## 1.2 Analysis of ongoing Research activities

The following table contains all security related FP6 projects, which have been categorized to highlight their research themes and main focus with respect to the STF Initiatives.

| 1.2.1.1 STF Initiative | WSI | IISI | ASI | DTI | BSI | IPI | DAMI | CRI | SPI | SRI | MScI | SVPI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Project** | | | | | | | | | | | | |
| **BIOSEC** | | | | | ** | | | | | | | |
| **e-JUSTICE** | ** | | | | * | * | | | * | | | |
| **INSPIRED** | ** | | | | | | | | * | | | |
| **PRIME** | | | | | | ** | | * | * | | | |
| **SECOQC** | | | | | | | | ** | | | | |
| **SEINIT** | ** | * | * | * | | | | | | * | * | |
| **ECRYPT** | | | | | | | * | ** | * | | | |
| **FIDIS** | | | | | | ** | | | * | | | |
| **BioSecure** | | | | | ** | | | | | | | |
| **Digital Passport** | | | | | ** | * | | | | | | * |
| **MEDSI** | | | ** | | | | | | | | | |
| **POSITIF** | | | | | | | | | ** | | | |
| **SCARD** | | | | | | | | ** | | | | |
| **SECURE JUSTICE** | | ** | | | * | * | | * | * | | | * |
| **SECURE PHONE** | * | | | | ** | * | | * | | | | |
| **LOBSTER** | | | | | | | | | | ** | | |
| **NOAH** | | | | | | | | | | ** | | |
| **MOSQUITO** | * | * | * | ** | | | | | * | | * | |

**Table 1:** Categorisation of FP6 Security Projects into Research Themes

**Table Key:** double asterisk denotes the major field of security research and the black asterisk denotes sub-security research fields as a consequence of the major research field. *Note: The projects in this table highlight the main areas of research that they are currently security focused. Some projects may touch on other research areas.*

This categorization will advance the roadmap being provided by SecurIST towards FP7. The table highlights key research areas and assists the SecurIST researchers to pinpoint areas that still need to be addressed.

Moreover, there are a number of interesting FP6 projects whose objectives are indirectly related to the Security and Dependability research thematic areas and those projects have also been mapped to the thematic areas in the following table.

| 1.2.1.2 STF Initiative | WSI | IISI | ASI | DTI | BSI | IPI | DAMI | CRI | SPI | SRI | MPSI | SVPI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Project** | | | | | | | | | | | | |
| **Daidalos** | ** | * | | | | * | | | * | | * | |
| **Simplicity** | ** | | | | | | | | * | | | |
| **MAGNET** | | | | | | ** | | | | | | |
| **iTRUST** | | | | ** | | | | | | | | |
| **UBISEC** | ** | | | | | | | | | | | |
| **WCAM** | ** | | | | | | | | | | | |
| **DIADEM FIREWALL** | | ** | | | | | | | | | | |
| **INSTINCT** | ** | * | | | | | | | | | | |
| **SEMANTIC HIFI** | | | | | | | ** | | | | | |
| **EMAYOR** | | * | ** | | | | | | | | | |
| **WIDENS** | ** | | | | | | | | | | | |
| **WWIAmbientNetworks** | ** | | | | | | | | * | | | |
| **GUIDE** | | | | | | ** | | | | | | |
| **CI$^2$ RCO** | | * | | | | | | | | ** | | |
| **GST (e-Safety)** | | * | * | | | * | | | | | | ** |

**Table 2:** Categorisation of indirect Security related FP6 Projects into Research Themes

**Table Key:** double asterisk denotes the major field of security research and the black asterisk denotes sub security research fields as a consequence of the major research field. *Note: The projects in this table highlight the main areas of security research that they are currently focused on as a by-product of its primary objective. This table is not exhaustive and conveys a subset of FP6 projects integrating security features.*

## 1.3 Themed Workshop outcomes

The challenge for the Security and Dependability community is to identify the priorities and interrelationship between these areas. In the communications community, we are already aware of the challenge in trying to create a common communications platform, which can support the convergence of the IT and telecommunications infrastructures. The challenge for the security industry is much more complex requiring greater synergies between security research activities in the areas identified above in the initiatives.

The SecurIST project is attempting to achieve a degree of consensus by bringing together lead players in these areas under the Security Taskforce. The approach is the establishment of themed working groups under the taskforce charged with the task of contributing to the development of a security and dependability road map to support future ICT security requirements. The emphasis is on developing common research links between the various themed areas.

The objective of the Inaugural and 2$^{nd}$ Workshop was to establish the Working groups and start identifying the key challenges to contribute to the categorisation research of priorities, and specifically address the issues relating to the development in the Security and Dependability domain for the Seventh Framework Programme.

The Workshops achieved these objectives via the following:

1. Presentations of the STF Initiatives Terms of Reference,

2. Presentations of EC funded Security and Dependability related projects with a focus on key challenges,

3. Guest Speaker presentations on various themes of relevance to the STF Initiatives, again focusing on key challenges.

The following contains a consolidated summary of the challenges and potential for FP7 shown for each of the Initiatives as presented at both the Inaugural SecurIST Workshop and the Second Workshop.

**Dependability and Trust Initiative**

- Trends for huge networked computer systems are likely to become pervasive, as information technology is embedded into virtually everything, and to be required to function essentially continuously. Even today's "best practice" will not suffice for such systems. Therefore, enhanced “best practices” are needed.
- Much further research is required on all four technologies (fault prevention, removal, tolerance, and forecasting), aimed at making dependability and security into a "commodity" that industry can value and from which it can profit (through offering warranties on security and dependability of software and systems).
- Need for a system (not just software) development approach, which enables the likely impact on system dependability and security of all design and deployment decisions and activities to be assessed throughout the system life cycle, and caters for system adaptation, and the realities of huge, rapidly evolving, pervasive systems.
- Quality assurance measures to incorporate forecasting risk management strategies (transparency and comparability), trust management strategies (dynamic relationships), mitigation schemes, incident detection and incident management schemes (correlation for detection/monitoring).
- New context aware systems against spoofing, denial of service (dos), authentication.
- Reconciling uncertainty with predictability, managing apriori undefined or evolving failure modes and system configurations, management of exposure, interdependence and interference, handling of operation mistakes and unskilled users, adaptation to fault/attack ranges: from script kids to cyber terrorists; low to high-power attackers; benign to harsh environments.
- More research is needed in reference Models / Architectural frameworks for enabling Resilience and Generic Architectures for Dependable/Trustworthy/Resilient Systems.
- Building of Trust - merging several ranking and integration of security mechanisms.
- Multi-layer, transversal architecture, Trusted components.

**Security Policy Initiative**

- There is a need for uniform/common descriptions of involved technologies
- There is a need for multi- and mixed- level policy languages

- There is a need for policy manipulation / refinement and integration of policy languages with other domains (e.g. QoS)
- There needs to be a system description for basic functionalities, library of components and node mobility / reconfiguration needs to be possible to keep account of the dynamic changes that are happening to the system
- There is a need for automatic tools for policy management, deployment and control to enable simulation (technical and economical) and optimization, synthesis and verification
- The current "on/off" type of security measures and trust relationships are no longer applicable. Corporations will need to look into new ways to describe trust relationships and how to keep these descriptions dynamically up-to-date. We are looking here at solutions that go far beyond what "identity management" currently covers, and again we will need to look at solutions that integrate layers of security policy enforcements, incident management as well as policy update schemes. In short, the whole life cycle of security needs to be integrated to enable safe and secure SW development.

**A1.3 Wireless Security Initiative**

- Secure neighbour discovery:
  - MIPv6 and AAA integration.
  - Interdomain issues.
  - Key management.
- Security in sensor and ad hoc networks.
- Standardisation is a major contributor for security functions but there are areas not within the scope of standardisation that needs further investigation (e.g. network design, protection of network nodes, security analysis of IETF protocols in the 3G context).Regulatory aspects
  - Lawful interception
  - Anti-fraud policy
  - Regional policy
  - Privacy
- Research in Access and Smart Cards/USIM/ISIM very important.
- Global Identification vs. Context-specific local recognition. Moving from persistent identification to context adaption is a critical aspect in making technology adapt to people instead of forcing people to adapt to badly designed technology. It is easier and less invasive to change technology than it is to change people.
- Eliminate the dependence of compliance management to focus on sustainable security through citizen empowerment (database silos vs. persistent logical identity boundaries determined by context).
- Implementing Security by Design e.g. RFID security - Authenticity against product counterfeiting, data security through Owner control and convenience through context-specific keys can be built-in by carefully redesigning even these low-computational RFID-chips.
- Creation of one Citizen ID key device.
- Compliance management cannot replace security.

- Using Security by Design with European values as basis for Next generation infrastructure and ambient computing. This is technically difficult and involving many disciplines.
- There is a lack of quality research and understanding of the dynamics of Trust Socio/Economics (Security everywhere is designed assuming citizen security and "privacy" can be left to regulation and compliance management leading to bad design based on increasing Global Identification eroding both security and trust).
- The lack of skilled people will be a serious barrier to the necessary change as almost no existing ICT standards are secure enough for the fully linked Information Society.
- Infrastructure design approach must move away from customer lock in.
- Project "Privacy Highway" is an attempt to overcome this serious skills shortage by securing critical infrastructure. The foreseen outcome is the theoretical and eventually also deployed elimination of trade-offs between security, privacy, convenience and efficiency in normal society processes providing a structure and model for re-establishing trust with substantial socio/economic innovation and growth benefits.
- Ambient intelligence security.**Security Research Initiative**
- Providing trust by guaranteeing security and privacy through different channels covering regulatory and policy issues, data protection, identity management and defining appropriate standards and guidelines.
- Awareness creation among the users and facilitating the easy understanding of ambient intelligence and security levels required for different communication needs.
- Threats and vulnerabilities have to be identified and should be addressed based on level of security needed and user/application profile in an auto configuration mode, so that users get more trust in the network and applications. Such functionality will raise the trust among the users.
- Risk mitigation solutions (e.g. IT-Security protection measures and network & service availability) needs to be integrated on many layers.
- Addressing the users (citizens, business and Govt. organisations) requirements, usability criteria, available resources, market trends and identifiable gaps in providing pervasive trust among users. Based on such analysis, security architecture and protocols will be studied towards developing the security research framework.
- Better understanding and Identification of Zero Day worms.

**Applications Security Initiative**

- Secure code development
- Source code analysis
- Scalable application level computing systems
- Application compliance and measurement quality
- Enabling always-on mobile security
- Enabling mobile privacy
- Enabling security across virtual organisations (GRID, eScience, …)
- Protection against viral epidemics at Application level (DDoS, Malware, etc,)
- FOSS: free open source software will be a major player in future
- Open Source Software Application Development
- Benchmarking Open Source Software

- Security Issues of Open Source
- Tackling critical web application security flaws (see www.owasp.org)
- Application testing frameworks
- Easy to use (user interface) and management systems for application security.

**Internet Infrastructure Security Initiative**

- How IPv6 integration and deployment will affect the security of a network.
- Secure Internet technologies.
- Defending Internet protocol code exploits (e.g. buffer overruns).
- Scaleable Internet security technologies across different environments.
- Enabling always-on mobile security.
- Enabling Internet privacy.

**Identity and Privacy Initiative**

- Compatibility (Standards)
- Increasing laws and regulations (enforcement, forensics)
- Societal changes (privacy behaviour)
- New identity and privacy challenges within mobile applications (there will be synergies with the Wireless Security and Biometric Security Initiatives):
    - User policy driven (determined) and privacy friendly access control,
    - graceful integration,
    - secure identity carrier beyond the chip card or SIM,
    - careful evaluation of biometric patterns and mechanisms and application areas growing beyond the standard mobile communication domain.
- There is more research needed on psychological aspects of privacy and identity issues (i.e. research on perception vs. reality or how do people behave when they are in control of security and privacy mechanisms vs. being out of control).

**Biometrics Security Initiative**

- Robustness
- Trust in biometrics
- User-centred issues:
    - Legal framework
    - Data protection
    - Identify acceptance barriers
    - Privacy security perception
    - Usability
    - Convenience

  - Cross-European studies
  - Education
- Technical:
  - Multimodal biometrics
  - Aliveness detection
  - Likeness detection and linking presence
  - Robustness
  - Secure Storage
  - Network authentication
- Certification:
  - Evaluation of performance
  - Interoperability
  - Security
- Improving biometric authentication to minimize false positives
- Need to develop reliable biometric recognition algorithms that permits authentication on-card.
- Need to overcome on-card limitations (limited storage, restricted language, biometric authentication must be on card).

**Security Architecture and virtual Paradigms Initiative**

- Intelligent Fixes & Failure Recovery Policies Enactment.
- Understanding the prevalence of critical vulnerabilities over time in the real world is very important. The shortening of half-life of external and internal vulnerabilities is very important. There will be change of security paradigms necessary from perimeter protection to the holistic integrated system security, from central access controls to de-centralized usage control, from patch management on demand to long term sustainable security, from security as a product to security as a dynamic process.
- End to end layered security architectures.
- Security guidelines, Adapt the system to the user.
- Telecommunication networks are being increasingly viewed within a mobile applications-centric business context to be supported by grid-enabled service-oriented architecture. Thus, dynamic S&T services provisioning faces challenging connectivity, inter-operability, resourcing and security requirements for example: Security-risks-context-specificity and business-logic-compatibility of:
  - Secure scalable dynamic identity, privacy and trust chain management (AAA) and single-sign-on including incremental deployment of encryption and multi-factor bio-metrics security measures only as necessary to accommodate AAA including pseudonyms, anonyms, federated identities, dynamic roles/rights (also of non-observability), DRM, and ad hoc team/network support
  - Distributed, testable, re-adaptive and knowledge-integrative QoS-aware security services. These services are to include layered context-aware behaviour-

based models to facilitate socially intelligent secure user delegation to smart proxies within a framework for Personalise-able Privacy and Trust enhancing technologies (PETS). Such PETS are to deploy user advocacy-delegation services, user security knowledge management support and secure e-services bundling, SLA negotiation, contracting, e-billing and e-ticketing.

- Addressing the needs to deliver Framework Solutions Architectures for security enhancement and its testability and diffusabilty evaluation with the following attributes:
    - Holistic approach (less piecemeal)
    - More of capacity enhancing for security protection
    - Socially intelligent
    - Rich Layered Context-aware, Behaviour-Based Models
    - Scalable, QoS_aware, secure user delegation
    - Layered (models), distributed, flexible, knowledge-integrative
    - entirely new class of middleware needed
    - Adhoc team/network supportive, Re-Adaptive.

**Methods Standards Certification Initiative**

- Is the standards development process able to change and respond to the new changing paradigm on current challenges to the Security and dependability community, which can be summarised by:-
    - 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.
- The need to shorten time it takes to develop a consensus on a standard within the ISO world.
- Need to address the lack of participation from the user community, especially from SME sector.
- Security and dependability issues are the concerns of all the standards organisations but the liaisons between them are not always clear cut, and visibility on the issues being worked upon is not always available when needed.

**Cryptology Research Initiative**

- When we evolve to an *ambient intelligent world*, privacy concerns will increase and cryptology will need to be everywhere (even in the smallest devices).
- Cryptology will be needed that can offer acceptable security and performance at very low cost (hardware footprint, power consumption).
- Cryptology will be needed to distribute trust and to reduce the dependence on a single node.

- Advanced cryptographic techniques need to be developed that can offer protection against denial of service and spam (“proof of work techniques), robustness against intrusions and compromise (“distributed trust” for election schemes and for networks).
- Encryption for larger storage.
- Cryptography techniques for long-term security of highly sensitive data e.g. 50+ years.
- Resisting mathematical advances and quantum computers potential for breaking schemes in future.
- Need for advanced techniques for watermarking and perceptual hashing. In this area, there is also a strong need for better models and definitions.
- Overall, there is a very strong need to expand and strengthen an approach that takes into account rigorous models and provable security.

# 5 Conclusion

In conclusion, this paper's purpose is twofold. It will serve as an introduction to the thematic areas already identified for the strategic research agenda of FP7 and incorporates the results of the SecurIST Inaugural Workshop, which was held in January 2005 and the second workshop, which was held in April 2005.

## References

[Secu04] Security Taskforce Repository: http://www.securitytaskforce.org/
[Eict04] "Strengthening Competitiveness through Co-operation", European Research in Information & Communication Technologies, Brussels, September 2004
[Eura04] "EU in discussion over 2010 ICT objectives", November 2004, www.euractiv.com
[Tilm05] Tilman Vincent, "Challenges for Europe's Information Society Beyond 2005", Eurochambres, January 2005.
[FiCll05] Fitzgerald William, Clarke James, "SecurIST Inaugural Workshop Proceedings" report January 2005, http://www.securitytaskforce.org/
[ClFi05] Clarke James, Fitzgerald William “SecurIST 2nd Workshop on ICT Security & Dependability Research Strategy" report January 2005, http://www.securitytaskforce.org/