SIXTH FRAMEWORK PROGRAMME
PRIORITY 2
Information Society Technologies

COORDINATION ACTION

SecurIST 2nd Workshop

On

ICT Security & Dependability Research strategy

Date: 19th April 2005
Time: 09:30 – 17:30 CET
Centre de conferences, Albert Borschette, ROOM 4D, 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/050419/M/v0.1
Project Document Date: 16/05/2005
Workpackage Contributing to the Project Document: WP1
Deliverable Type and Security: R[1]-CO
Author(s): Jim Clarke, Will Fitzgerald, Miguel Ponce De Leon, Willie Donnelly, Latif Ladid, Speakers provided summary descriptions of their individual speeches in Annex 2.

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

Table of Contents

0. Executive Summary

The primary goals of the second SecurIST workshop were:

- Launch of the Security & Dependability Task Force (STF)
- Build the STF Initiatives and discuss their terms of reference
- Outline the skeleton of the strategy roadmap for call 5/6/FP7 and Beyond 2010
- Begin detecting linkages, dependencies and harmonisation between the Initiatives
- Set the milestones and achievements for the next 6 months.

The contributions from the six (6) guest speakers and the eleven (11) STF initiatives chairs have reinforced the great value of this global security initiative in many areas for the benefit of the European industry and society. The notions of societal impact, end-user centricity and the global outreach of the security initiatives, have been addressed right from the outset, adding the needed dimensions to the Task Force.

The STF workshop has attracted a distinguished audience from policy-making, industry, research and academia positioning the strategic significance of this work at its proper level and setting the expectations for a very positive and high quality level of work and outcome.

The schedule set for the production of the Documents For Comment (DFC) by the 11 STF initiatives calls for three releases: DFC-01 for end of 15th June, 2005. DFC-02 for 15th September, 2005 and DFC-03 for 15th October, 2005, which will be the milestone for the next STF meeting in Brussels on 18th October 2005. DFC-01 will be prepared in view of the STF Advisory Board meeting planned for 27th June, 2005.

This document provides a brief overview of the STF and the proceedings of its 2nd workshop on ICT security and dependability research strategy. It's the basis for the production of the first DFC (DFC-01) for each initiative. Companies and projects wishing to join this initiative can register their interests at www.securitytaskforce.org

We look forward to your participation.

Dr. Willie Donnelly, SecurIST project manager

1. SecurIST Second workshop Proceedings

1.1 Opening session and introduction of the European Security & Dependability Task Force Workshop

by Dr. Willie Donnelly, Waterford Institute of Technology

The purpose 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:

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

The Strategic Research Agenda to be developed by the Security Taskforce will elaborate the ICT Security & Dependability Research strategy beyond 2010. It will provide Europe with a clear European level view of the strategic opportunities, strengths, weakness, 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.

The work of the taskforce is organised into work groups called initiatives. Each initiative is charged with bringing together security experts in a particular technical domain to develop consensus on the research priorities to be addressed within the Strategic Research Agenda.

The second SecurIST workshop formally established the taskforce and set out its terms of reference. The workshop offered the initiative leaders an opportunity to present their initial views on the research challenges to be addressed within the strategic research agenda to the wider taskforce members. The emphasis of the SecurIST project in organising its workshops is to broaden the security debate to incorporate trans-disciplinary security requirements through dialogue between the various initiatives.

A key element of the SecurIST workshop is the delivery of keynote presentations by internationally known security experts. These presentations are designed to stimulate debate and provide the taskforce members with a broad appreciation of security issues across the entire ICT domain.

Following the results of this second workshop, the taskforce is now in a position to deliver an initial security technology roadmap by the middle of the summer 2005. This will be disseminated to the wider security community in industry, academia and government for comment with the final aim of producing input to the EU 7th framework work programme.

These proceedings provide details of the Security Task Force initiatives and an overview of the workshop presentations and conclusions.

1.2 Security Task Force Initiatives. Terms of References

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 under the umbrella of the Security and Dependability Task Force (STF). The following contains a description of the Terms of References (areas they cover) of the Initiatives.

A listing of the registered members of the individual Initiatives can be found in Annex 1. More detailed information on the individual initiatives can be found in Annex 2. Summary of Presentations.

Dependability and Trust Initiative (DTI) Terms of Reference: 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): Focusing on research in policy-driven security in the areas of languages and tools and policy-based applications. This approach will let managers concentrate on high-level rules rather than implementation details and provide auditors with a formal specification for measurements.

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): This initiative is engaged in linking results of different research groups and initiatives into one cohesive vision for the European research and development strategy addressing security and privacy in ICT such as innovative network security architecture and models, 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) and common security framework for both wireless and wireline architectures.

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

Identity & Privacy Initiative (IPI): Research focusing towards digital identity management, privacy protection and mediation, personal data environments and other privacy enhancing technologies, privacy and authentication within fixed and mobile/wireless environments.

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. 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.

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 communicating domains and their enclosures to allow S&T services selection, composition and matchmaking. 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).

The expected result of the MSc Initiative would be to initiate actions leading to the improved awareness of, participation in and take-up of security standards. This could be shown by a measurable improvement of training and certification in security standards of European companies, products and personnel.

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.

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.

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.

STF Initiative	WSI	IISI	ASI	DTI	BSI	IPI	DAMI	CRI	SPI	SRI	MPSI	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.

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 Outcomes of Workshop

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 2nd Workshop was to continue the work which began with the Inaugural Workshop held in January 2005. The output from the workshops will contribute to the categorisation research of priorities, and will specifically address the issues relating to the development in the Security and Dependability domain for the Seventh Framework Programme.

The Workshop 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 by their central themes as presented at both the Inaugural SecurIST Workshop and the Second Workshop.

Dependability and Trust:

- 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:

- 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.

Wireless Security:

- 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:
- 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:
- 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:

- 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 management:

- 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:

- 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:

- 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 decentralized 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:

- 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.

1.4 Setting Security and Dependability Priorities (2006 – 2010)

The main target of the STF is to assist in the developopment of the European Security and Dependability framework and strategy to follow. The process involves multiple threads:

- Participation of stakeholders (STF and Advisory board)
    - Political, regulatory and policy issues to be addressed
- Close links to Standards, Forums and related national initiatives
- Contribution of IST projects and other experts: Main issues, gaps analysis
    - Where we are – State of the Art?
    - Where we want to go ?
    - Identify Gaps/barriers/challenges
- Awareness creation
    - Communication across the industry, vendors, users and forums.

The strategy is to continue to recruit experts in each of the initiatives as required and develop a vision (top-down approach) and identify what we have and identify gaps (bottom-up approach from IST projects and other experts). The next step will be to develop documents for comments (DFCs) to obtain concensus on the framework taking into account relationships and dependencies with other initiatives in order to build a consistent framework to recommend the European Research priorities.

The schedule set for the production of the Documents For Comment (DFC) by the 10 STF initiatives calls for three releases:

- DFC-01 for end of 15th June, 2005. DFC-01 will be prepared in view of the STF Advisory Board meeting planned for 27th June, 2005.
- DFC-02 for 15th September, 2005.
- DFC-03 for 15th October, 2005, which will be the milestone for the next STF Workshop in Brussels on 18th October 2005.

Annex 1. Security Task Force Initiative Membership

A1.0 Introduction

This Annex contains a listing of the members of each of the Security Taskforce Initiatives. The information is comprised of the Acting Leader of the initiatives and the names and organisations of the registered members[2] of the Initiatives.

Please note that the STF Initiatives are still actively recruiting new members. If interested in registering, we request that you do both of the following:-

1. Register on-line for the initiative(s) of interest at www.securitytaskforce.org.
2. Contact and introduce yourself to the Initiative leader directly with the email(s) given below.

A1.1 Dependability and Trust Initiative (DTI)

Initiative Acting Leader:

Name	Organisation	Contact email
Paulo Verissimo	FCUL[3]	pjv@di.fc.ul.pt

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Tom Anderson	University of Newcastle upon Tyne
Roberto Baldoni	Dipartimento di Informatica e Sistemistica - Univ Roma
Andrea Bondavalli	Dept : Design and Analysis of Computer Systems - DACS
Karima Boudaoud	Laboratoire I3S-CNRS
Christian Cachin	IBM Research Zurich
Miguel Castro	Microsoft research
Marc Dacier	Eurecom
Yves Deswarte	LAAS-CNRS in Toulouse, France.
Sofoklis Efremidis	INTRACOM S.A.
Nuno Ferreira Neves	Faculdade de Ciências da Universidade de Lisboa
Alfred Gottwald	Siemens
Bernard Hämmerli	Acris GmbH und HTA Lucerne University of Applied Science
Jörg Kaiser	University of Ulm
Miroslaw Malek	Humboldt-Universität zu Berlin
Fulvio Marcoz	Finmeccanica
Refik Molva	Eurecom
Simin Nadjm-Tehrani	Linköping University
Ludovic Pietre-Cambacedes	EDF
David Powell	LAAS-CNRS in Toulouse, France.
Brian Randell	University of Newcastle upon Tyne
Luca Simoncini	Department of Information Engineering- University of Pisa
Ines Vidal	Euskaltel, S.A.
Konrad Wrona	SAP Labs France
Neeraj Suri	TU Darmstadt, Dept. of Computer Science
Paulo Verissimo	FCUL[4]

[2] Registered as of 19th April 2005 on www.securitytaskforce.org.
[3] Faculdade de Ciências da Universidade de Lisboa
[4] Faculdade de Ciências da Universidade de Lisboa

A1.2 Security Policy Initiative (SPI)

Initiative Acting Leader:

Name	Organisation	Contact email
Antonio Lioy	Politecnico di Torino	lioy@polito.it

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Tobias Christen	Stonesoft
Ulf Hägglund	Smarticware AB
Alfred Gottwald	Siemens
Ulf Hägglund	Smarticware AB
Antonio Lioy	Politecnico di Torino
Antonio F. Gómez Skarmeta	Universidad de Murcia - Spain
Konrad Wrona[5]	SAP Labs France

A1.3 Wireless Security Initiative (WSI)

Initiative Acting Leader:

Name	Organisation	Contact email
Bosco Eduardo Fernandes	Siemens	bosco.fernandes@siemens.com

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Stephen Butler	LAKE Communications
Stephan Engberg	Open Business Innovation
Bosco Eduardo Fernandes	Siemens
Antonio F. Gómez Skarmeta	Universidad de Murcia - Spain
Stephen Hailes	UCL
Christian Hauser	University of Stuttgart
Maria Karaguiozova[6]	Infineon Technologies
Javier Lopez	UNIVERSITY OF MALAGA
Anuar Mohd	USM
Erik Norgaard[7]	Atos Origin
Mícheál Ó Foghlú	Waterford Institute of Technology
Riccardo Pascotto	T-Systems International
Anna Plataki[8]	Infineon Technologies

[5] Can provide details for MOSQUITO contact in this area.
[6] Registered for SCI, which is now merged with WSI.
[7] Registered for SCI, which is now merged with WSI.
[8] Registered for SCI, which is now merged with WSI.

A1.4 Security Research Initiative (SRI)

Initiative Acting Leader:

Name	Organisation	Contact email
Sathya Rao	Telscom	rao@telscom.ch

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Uwe Bendisch	Fraunhofer Institute for Secure Information Technology
Anestis Filopoulos	Digitalis Consult
Ulrich Friedrich	Atmel
Mathieu Gorge	VigiTrust
Thomas Haeberlen	ENISA - European Network and Information Security Agency
Michael Kreutzer	Darmstadt University of Technology
Evangelos Markatos	FORTH (Foundation for Research and Technology - Hellas)
Tom McCutcheon	Dstl
Sathya Rao	Telscom
Mark Reilly	Enterprise Ireland
Reijo Savola	VTT Technical Research Centre of Finland

A1.5 Application Security (ASI)

Initiative Acting Leader:

Name	Organisation	Contact email
Jim Clarke	Waterford Institute of Technology	jclarke@tssg.org

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Alberto Bianchi	Marconi-Selenia
Oscar Blanco	Ericsson
Jim Clarke	Waterford Institute of Technology
William Fitzerald	Waterford Institute of Technology
Gerardo Lamastra	Telecom Italia - TILAB
Patrick Sinz	Ethiqa SAS
Simela Topouzidou	Athens Technology Centre
Konrad Wrona[9]	SAP Labs France

A1.6 Internet Infrastructure Security Initiative (IISI)

Initiative Acting Leader:

Name	Organisation	Contact email
Miguel Ponce de Leon	Waterford Institute of Technology	miguelpdl@tssg.org>

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Oronzo Berlen	Getronics
Stephen Butler	LAKE Communications
Latif Ladid	Independent consultant
Miguel Ponce de Leon	Waterford Institute of Technology
Patrick Sinz	Ethiqa SAS
John Ronan	Waterford Institute of Technology

[9] Can provide details for MOSQUITO contact in this area.

A1.7 Identity and Privacy Initiative (IPI)

Initiative Acting Leader:

Name	Organisation	Contact email
Kai Rannenberg	Goethe University Frankfurt	kai.rannenberg@m-lehrstuhl.de

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Kajetan Dolinar	SETCCE
Marit Hansen	Independent Centre for Privacy Protection Schleswig-Holstein, Germany
Christian Hauser	University of Stuttgart
David-Olivier Jaquet-Chiffelle	University of Applied Sciences of Bern
Henry Kraseman	Independent Centre for Privacy Protection Schleswig-Holstein, Germany
Alexandra Michy	SAGEM
Martin Neubauer	University of Stuttgart
Kai Rannenberg	Goethe University Frankfurt
Stefan Weiss	Deloitte and Touche

A1.8 Biometrics Security Initiative (BMI)

Initiative Acting Leader:

Name	Organisation	Contact email
Orestes Sánchez-Benavente	Telefónica I+D (TID)	orestes@tid.es

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Henning Arendt	@bc
Alexandra Michy	SAGEM
Erik Norgaard	Atos Origin
Aljosa Pasic	ATOS Origin
Silvia Renteria	ROBOTIKER-TECNALIA
Orestes Sánchez-Benavente	Telefónica I+D (TID)
Kush Wadhwa	International Biometric Group (UK)

A1.9 Security Architecture and Virtual Paradigms Initiative (SVPI):

Initiative Acting Leader:

Name	Organisation	Contact email
Atta Badii	University of Reading	atta.badii@reading.ac.uk

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Francois Armand	Jaluna
Atta Badii	University of Reading
Jerome Billion	Trialog
Bruno Crispo	Vrije Univeristeit Amsterdam
Jarkko Holappa	VTT Electronics
Peter Kirstein	University College London
Antonio Kung	Trialog
Alexandra Michy	SAGEM
Jan Weber	Omega Management Consultants
Patrick Sinz	Ethiqa SAS

A1.10 Methods Standards Certification Initiative (MScI):

Initiative Acting Leader:

Name	Organisation	Contact email
Alan Husselbee	ISSA (association running the CISSP certification)	ahusselbee@paris.com

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Jim Clarke	Waterford IT
Bosco Eduardo Fernandes	Siemens
Alan Husselbee	ISSA (association running the CISSP certification)
Sadhbh McCarthy	Local Government Computer Services Board
Tim Willoughby	Local Government Computer Services Board
Luc Van den Berghe	CENORM

A1.11 Digital Asset Management Initiative (DAMI):

Initiative Acting Leader:

Name	Organisation	Contact email
None[10]		jclarke@tssg.org[11]

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Shay Adar	M-Systems
Omid Aval	Smarticware AB
Adrian Waller	Thales Research and Technology (UK) Ltd.

A1.11 Cryptology Initiative (CRI):

Initiative Acting Leader:

Name	Organisation	Contact email
Bart Preneel	K.U.Leuven (Belgium)	Bart.Preneel@esat.kuleuven.ac.be

Current Membership: The following have registered via the SecurityTaskforce.org web site.

Name	Organisation
Fatih Birinci	TÜBITAK-UEKAE - National Research Institute of Electonics and Cryptology
Andrew H. Kemp	University of Leeds
Alexandra Michy	SAGEM
Bart Preneel	K.U.Leuven (Belgium)
Selçuk Taral	TÜBITAK-UEKAE - National Research Institute of Electonics and Cryptology

[10] No volunteers.
[11] Contact if you have an interest in leading this initiative.

Annex 2. Summary of Plenary Presentations.

A2.0 Introduction

This Annex contains a detailed description of the presentations made during the 2nd STF Workshop during the Plenary session of the Security Task Force Initiatives. The purpose of the session was twofold:

1. An opportunity for the Initiative leaders to present the Terms of reference of their Initiatives developed since the Inaugural Workshop and their registered members;
2. An opportunity to have invited Guest speakers to present their work within relevant STF Initiatives sessions.

A2.1 Dependability and Trust Initiative (DTI)

Presentor: Professor Brian Randell, University of Newcastle Upon Tyne, for Prof. Paulo Verissimo, FCUL.

In general, in line with the DTI's Terms of reference, what is needed is some combination of dependability and security. In particular, any security mechanisms must themselves be dependable - indeed most security breaches are due to dependability failures. Technologies for achieving dependability (both of systems, and of the system design process) and security can be classified into: fault prevention (rigorous design), fault removal (verification & validation) and fault tolerance (whose effective combination is crucial), and fault forecasting (system evaluation), the means of assessing progress towards achieving adequate dependability and security. In general, all four technologies are needed.

The fundamental threats to achieving dependability and security, i.e. to minimising the frequency and severity of system failures (of whatever kind) are faults, errors and failures: a system failure occurs when the delivered service deviates from fulfilling the system function; an error is that part of the system state which is liable to lead to subsequent failure; the adjudged or hypothesised cause of an error is a fault. Note that error does not necessarily lead to failure, failures do not necessarily constitute faults. These three essentially different concepts are needed because of the possibility of complex badly-specified systems, with uncertain boundaries, where judgements as to possible existence, causes or consequences of failure are difficult, and provisions for preventing faults from causing failures are likely to be fallible, i.e. with reality! It is usual to say that the dependability of a system should suffice for the dependence being placed on that system. The dependence of system A on system B thus represents the extent to which system A's dependability is (or would be) affected by that of System B. The concept of dependence leads on to that of trust, which can very conveniently be defined as accepted dependence. (All these and many more terms and concepts are defined in: Aviziienis, laprie, Randell & Landwehr: Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, 2004.)

Techniques and tools available today make it possible to produce complex computer systems that work adequately dependably and securely. However, there is a huge "deployment gap", with many organisations attempting to produce complex systems and in particular software using technical and management methods which are far from "best practice". Present trends indicate that 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.

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. The target is for those involved in creating future complex networked systems to find it technically

feasible to offer warranties on the dependability and security of their software and systems. This can be facilitated by means of 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.

A2.2 "Context-aware Security and Trust"

Presentor: Konrad Wrona, SAP Labs France

The MOSQUITO (IST-2002-506883) project, is a STREP project under EU Framework Program 6, which aims at developing a framework for implementing secure and adaptive business applications for mobile workers. Such applications would rely to great extent on various types of context information in order to adapt both its logics and its security measures.

In particular, within MOSQUITO, we differentiate between secure context-awareness, which focuses on ensuring availability, authentication, integrity and confidentiality of context-aware information, and context-aware security, which focuses on using context information in order to optimise and adapt security measures employed within distributed business applications.

The context information utilised for the context-aware computing can vary substantially, e.g. it can describe computing and physical environment, time, and user's state. It can also differ in regard to its persistence (e.g. static, dynamic), origin (e.g. internal, external), and quality (e.g. timeliness, coverage, resolution, and accuracy).

One of the challenges in distributed systems is the aggregation of context data from different providers. In particular, we have to consider malicious parties trying to provide false date in order to influence the final result of aggregation. Appropriate robust statistical methods and trust evaluation algorithms need to be but in place to ensure the trustworthiness of context information.

Context information can be used as input to many security-related processes, such as access control, authorisation and trust management. Context information can be used for (re-)configuration of security mechanisms, too. But looking at security in this space it is a trade off between optimisation and introducing new vulnerabilities.

Summarising, there are three main security challenges related to context-aware computing:

- Confidentially of context info
- Integrity of context info.
- Availability of the context info.

These three features have to be ensured in order to secure the new context aware systems against, e.g., context spoofing and DoS attacks. Secure context-awareness are fundamental for ambient intelligence. Also, privacy protection is an important, although often neglected, part of context aware applications.

During the first six months of execution of MOSQUITO we have achieved two main technical results:

1. Use case-driven engineering of functional and security requirements: During the initial phase of the project, we have defined three business use cases for the MOSQUITO platform. These use cases (i.e. fair deal, paperless car, and e-health scenario) are documented in the deliverable D1. They cover a wide area of business domains, and in particular they focus on such applications as insurance handling, car repair, medical advise, emergency situations, and contract negotiation. The scenarios have been developed in close collaboration with relevant business units of the industrial consortium members.

Based on our use cases we have extracted the appropriate functional and security requirements. A particularly interesting and challenging aspect of the requirements engineering was analysis of the security requirements. We have identified them by using the goal and anti-goal analysis. This approach has been selected after an in-depth study of several methods available in the literature. The use cases have been further used in order to develop an initial threats model, which will be extended and analysed in more detail in the later stage of the project, taking into account chosen technologies and implementation framework.

2. Initial design of context-aware trust and security architecture: Another important result of the first phase of the project has been an initial definition of the MOSQUITO architecture. In particular, we have developed a high-level design of context-aware trust and security (CATS) architecture, we have evaluated the relevant technologies, and we have defined appropriate collaboration models for adaptive mobile business applications. Our collaboration model is based on an innovative concept of distributed workflow management and constitutes a basis for further research and development activities in the later phases of the project. We have also performed a state of the art research on context awareness, which has resulted in early drafts of specifications for context-aware credentials, attributes, and CATS architecture.

After hearing all of the Initiatives presentations, we feel that, in addition to the Dependability and Trust Initiative, there are also good synergies between the MOSQUITO project and other initiatives, including Application Security Initiative and Security Policy Initiative, which will be further explored.

A2.3 Security Policy Initiative (SPI)

Presentor: Prof. Antonio Lioy, Politecnico di Torino

The presentation started with a definition of policy to clarify which definition was being examined by the SPI. There are two different meanings, one political and one technical. The two definitions for “Policy” are:-

•(political def)

–a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body

•(technical def)

–a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions.

The SPI is concentrating on the latter technical definition.

One of the principle issues that needs to be addressed is the lack of control over the technology descriptions. First there must be a common agreement on what we are speaking about. This is typically being done in the standardisation bodies DMTF and IETF regarding CIM / PCIM definition and extension and OASIS regarding RuleML (interoperation of policy languages).

You must have a system description as well as the security policy in order for the Policy Decision Point (PDP) to work correctly as shown in figure A1.3a.

In the current State-of-art, there are too many languages with different purposes / scopes (management, authentication, authorization, delegation, …). Some are generic, and there are some specific languages that are more target oriented. Some examples are PCIM

(CIM), Ponder (discontinued), XACML, SAML, Keynote, and ASL. There are Semantic languages, such as KAoS, RuleML, SWRL and Rei, which are not originally included as security oriented policy languages, but can be.

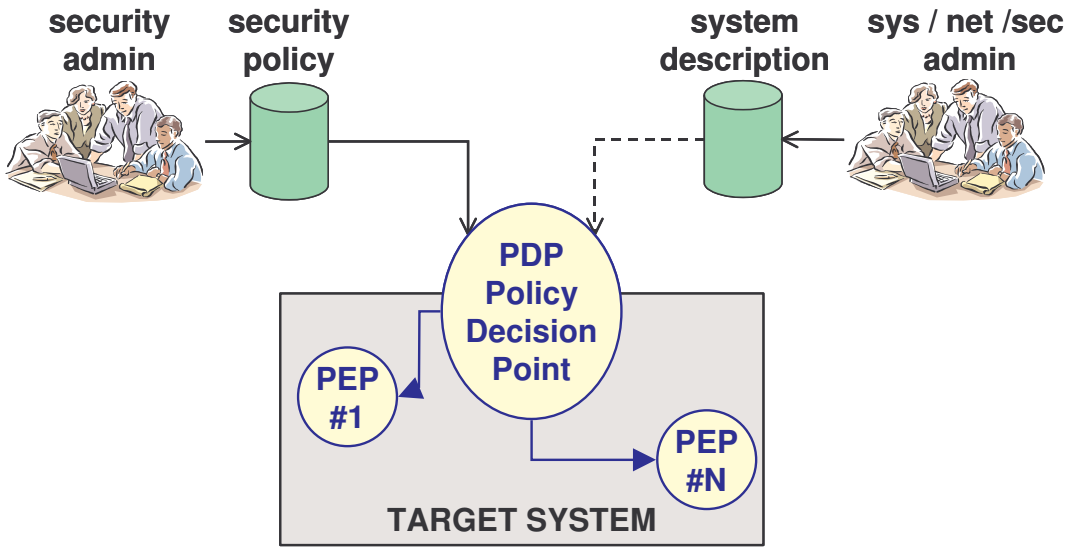

Figure A1.3a. High Level view

There are a number of challenges facing the SPI, including the need for multi- and mixed- level policy languages, need for policy manipulation / refinement and integration of policy languages with other domains (e.g. QoS). In addition, 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 registered participants to SPI include:-

- Politecnico di Torino
- University of Murcia
- WIT
- Stonesoft
- Siemens.

A2.4 “Toward a culture of security in Europe”

Presentor: Dr. Ronald de Bruin, European Network and Information Security Agency (ENISA)

Dr. de Bruin presented the ENISA, which is a Centre of expertise for network and information security. ENISA can give guidance to the European Commission and Member States and engages in information exchange and cooperation, raising awareness and dialogue with industry. ENISA’s role is to share best practice and they are involved in collection and analysis and then also disseminating and awareness. There is an increased

need for cooperation and information exchange and ENISA will bring the stakeholders together. It is foreseen there will be 38 people by end of 2005 and 44 people by 2006.

Dr. de Bruin presented the Working groups foreseen for this year and asked the participants to contribute to these if applicable. They are in the areas of Awareness Training, CERT Cooperation and Risk Management. The Call for interest for ad hoc Working Groups published at www.enisa.eu.int .

Dr. de Bruin presented ENISA's role within research programs:

- Modinis program (supports e-Europe 2005)
- ENISA studies planned for 2006
- FP7 / Security research program – input to development of research programme with ENISA expertise and dissemination activities.

In conclusion, it is recognised that network and information security affects everyone and does not stop at national borders or within specific sectors. ENISA shall contribute to creating a culture of network and information security. ENISA is in an intensive start-up phase and has begun its operational activities and it looks forward to cooperating with the network and information security community, including SecurIST.

A2.5 Wireless Security Initiative (WSI)

Presentor: Bosco Eduardo Fernandes, Siemens

This initiative targets security and dependability in Mobile/ Wireless service environments. It will address Ambient Radio, Ambient Networks and User Device capabilities in a 3G and beyond, Ad-hoc and All IP networks. It specifically focuses the Strategic Research Agenda for a Mobility Security in FP7 for:

- High level description of Mobility Security Framework
- Key security research priorities based on the Mobility realization
- Trustful Business Environment
- Security & Regulatory Framework Evolution
- Customer perspectives (USIM/Smart Cards)
- Security Framework Technologies & Research Topics
- Security as a Cross Issue of the Technology Platforms
- Identification of the relation with the other main activities of the Platform (e.g., joint trials may be appropriate).
- Content and applications
- Links to Standardization bodies and for a.
- Smart cards / USIM/ ISIM.

These include protocols, interfaces, Control, interoperability, Software, Stand alone systems and tools. The next steps for the WSI are:-

1. Identify Standards and other bodies dealing with subjects in the initiative.
2. Identified Challenges for 2006-2010. The gaps/challenges/bottlenecks.
3. Recruit new members/projects to WSI.
4. Provide input to preliminary White paper following workshop.
5. Draft the WSI document for comment (DFC).
6. Identify Interdependencies
7. Input to Call 5/Call 6/FP7/Beyond 2010.
8. WSI mailing list discussion (WSI@securitytaskforce.org with [WSI]).

The current registered participants to WSI include:-

- Siemens
- Atos Origin

- Open Business Innovation
- Universidad de Murcia - Spain
- University College London
- University of Malaga
- University of Stuttgart
- T-Systems International (Daidalos)

A2.6 "Wireless Device Id in the Ambient World - From Identification to Context Adaptable Recognition"

Presentor: Stephan Engberg, Open Business Innovation

Stephan Engberg addressed the ongoing change of security paradigm away from Global Identification towards context-specific local recognition. Context-specific identity is a Security by Design paradigm aiming to prevent risk - or from Bart Preneel presentation originating in the cryptographic understanding "You can trust it, because you don't have to trust it". The obvious reason is the present paradox that while risk acceptance in government and commercial environments are moving towards zero, we are assuming citizens will remain trustful. As trust is about risk acceptance in a world where individual security risks are concentrating, escalating and security breaches grow everywhere, trust is dropping fast and undermining the economy.

Focussing on the rapidly growing problem of Identity theft, Stephan Engberg demonstrated a causality analysis of the destructive arms race of the present security paradigm focussing. The growing distrust problem is self-imposed caused by Global Identification as the main driver of security risks and failures. Compliance management is doing nothing towards changing this. When security initiatives focus on more global identification it creates new dangerous sources of Identity Theft with increasing reversed burden of proof and also leads to destructive consequences such as abuse of pervasive surveillance and a economically trend towards digital feudalism monopolising individual consumer access to the increasingly digital world. Further, global identification push data security out of control due to concentrating risk in the rapidly growing databases leading to ever larger security failures, secondary abuse of data and data-based identity theft.

Among a long list of new "security" technologies worsening the security problems, he pointed to the assumption that biometrics will solve security problem. Biometrics must be considered spoofable in operational use, as it is globally identifying biometrics is creating new data security risks and worse creating security failures where criminals can walk through the security gates disguised as security-cleared personnel while the victims of biometrics-based Identity Theft might find themselves facing reverse burden of proof and blacklisted based on their non-revocable biometrics. Biometrics might just as well be fuelling the trust crises instead of reducing it putting serious question mark to for instance the haste of introducing digital passports without individual control of biometrics.

Instead, we are moving towards a new European-style security paradigm in line with the thinking in the FP7 strategy outline but taking a step further to eliminate the dependence of compliance management to focus on sustainable security through citizen empowerment. In order to enable the expected benefits of the Information Society, we need to replace the physical boundaries between silo-databases with persistent logical identity boundaries determined by context.

To exemplify the context-specific security paradigm in wireless device Id, he first addressed RFID security. He demonstrated how three main objectives; 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. The solution implements mutual recognition between the Consumer Device and the RFID-chip transparently across any transport layer. He then moved on to illustrate the Socio/economics and market potential of using Security by Design to incorporate security with European values.

Combating crime and distrust involve the need to focus on Security by Design moving away from Global Identification towards Local context-specific identity as the key enabler of the Information Society. As example he then addressed the issue of Mobile IP. To illustrate how Open Business Innovation is going to contribute to solving these problems, he pre-announced a series of key security solutions combining into what is required to talk about an Anti-Identity Theft wireless Life Management PDA/mobile phone. The list includes issues like instant revocability (by user), non-targetability (non-persistent HOME addresses in Mobile IP), context-specific accountability (one-way), context-specific addressability (receiver-controlled communication), individual control of biometrics and context-specific credit-payments among the key aspects. The purpose is to create one Citizen ID key device able to cover the full range of context-specific needs from transaction-anonymous location based services and digital cash transactions over consumer loyalty programs to eGovernment Healthcare and secure Digital Passports. An IT-system can never be more secure than the weakest link - user self protection.

Stephan Engberg re-iterated that Compliance management cannot replace security and that we in order to regain the lost trust need to move rapidly towards security that empower the citizen to protect himself against the many forms of identity theft and data abuse. Using Security by Design with European values as basis for Next generation infrastructure and ambient computing to remove the barriers for sharing information, we can release the growth potential to restore European competitiveness.

The biggest problem for security in the phase ahead is not technical, but the serious 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. We need to realise this and start teaching differently in both business schools and technical universities.

Second, as the list of issues addressed for Anti Identity Theft clearly illustrates, Security by Design is technically difficult and involving many disciplines. 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. Further there is no way around making security easy for the individual. 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.

As long as for instance mobile operators and payment intermediaries assume it is in their interest to create strong customer lock-in, security is eroded through infrastructure design, which is neither in the interest of infrastructure or society as such. We are all learning this the hard way in areas such as Identity Theft, RFID resistance and SPAM which are all self inflicted problems due to lack of attention to citizen empowerment and what that means in design terms.

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. In our view, these trade-offs are mere self-imposed illusions and therefore also solvable.

A2.7 "SecurePhone project"

Presentor: Erik Nørgaard, Atos Origin

Erik Nørgaard from Atos Origin presented the SecurePhone (IST-2002-506883), a STREP project under EU Framework Program 6. The SecurePhone project aims at bringing negotiation and signing of contracts into the context of the mobile communication, allowing the user to sign legally valid contracts on the fly independent of time, and place.

It is of fundamental importance for the acceptance of the device that signing documents is done in a natural and non-intrusive way. The SecurePhone project incorporates non-intrusive biometric authentication models: Face recognition, voice recognition and hand written signatures.

Hence, the SecurePhone will contain two pieces of confidential information: The private key for digital signatures and the biometric profiles of the owner. For the privacy and security of the owner, these data must remain under his/her control at all time.

To protect confidential data, these data are stored on a SmartCard, which has a proven record of security against tampering and a strong data access control. Any operation requiring access to these data must be done on the card to prevent the possible memory leak, ie. that confidential information becomes accessible to the intruder.

Currently available SmartCard based on the JavaCard platform supports strong cryptography natively. The main challenge of the SecurePhone project is to develop reliable biometric recognition algorithms that permits authentication on-card.

The SecurePhone project has considered a number of security problems in the design and development of the phone:

- Personal data must remain under control of the owner: Loss of the SmartCard should not imply loss of identity
- Biometric recognition models must be considered against the data we want to protect: We don't want users to risk being beheaded because a simple thief wants to make a phone call
- Private encryption key must remain private: Only the owner may access the private key for signing documents and the key must be revocable.
- Operation in a hostile environment: The security modules can not trust the other applications.
- Operations must be atomic: The card must not be left in a partially authenticated state, sessions should be avoided.

Current challenges:

- Improving biometric authentication to minimize false positives
- Developing methods for authentication that can be implemented on the card

The SecurePhone project aims at developing a proof-of-concept: That the idea is supportable by existing hardware and software platforms and given further development can bring secure contracts to the mobile user.

The SecurePhone project actively pursues the realization of the objectives of a number of initiatives under SecurIST, in particular:

- Biometry Security Initiative
- Identity and Privacy Initiative

- Wireless Security Initiative incl. Smart Cards

and can contribute to and/or benefit from these initatives. Other initiatives may become relevant as announced.

A2.8 Security Research Initiative (SRI)

Presentor: Dr. Sathya Rao, Telscom

The presentation of Dr. Sathya Rao provided an overview of the broader issues involved in security research initiative. The issues cover all layers across end to end communication link involving physical infrastructure security to application level security. The overall objective is to provide trust by guaranteeing security and privacy through different channels covering regulatory and policy issues, data protection, identity management and defining appropriate standards and guidelines. The usability of ICT will be only possible through 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 autoconfiguration mode, so that users get more trust in the network and applications. Such functionality will raise the trust among the users.

In developing vision for security research, the initiative will address 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. The vision documents will be developed in the form of 'document for comments (DFC)' that would be made available to all STF members so that the documents can be commented by IST project groups, national initiatives and experts. The document will be updated taking into account the different feedback, which may result into 'security research framework' document that can be used by the EU for developing the 'European strategic research area'.

A2.9 "Critical Information Infrastructure Protection"

Presentor: Uwe Bendisch, Fraunhofer Institute for Secure Information Technology (SIT)

The **Critical Information Infrastructure Research Co-ordination** (CI^2RCO) project is a so called Co-ordination Action co-funded under the Information Society Technologies (IST) Priority of the 6th Framework Programme by the European Commission (Project-No: IST 2004-15818, Time frame: March 05 – Febr. 07). The project addresses the creation and co-ordination of a European taskforce to encourage a co-ordinated Europe-wide approach for Research and Development (R&D) on Critical Information Infrastructure Protection (CIIP).

The aim of our modern human society is its safe, permanent and sustainable development. A Critical Infrastructure supports the orderly functioning of the society and economy at large. For that reason, it is of utmost importance that these Critical Infrastructures are both functional (efficient and powerful) and reliable.

Our society is nowadays heavily depending on Information and Communication Technology (ICT). ICT has pervaded in all traditional infrastructures, rendering them more intelligent but more vulnerable at the same time. Our new economy is highly dependent on

such critical and reliable information infrastructure services – they are to be considered as Critical Information Infrastructures. A disruption or destruction of those infrastructures would have serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments. Survivability and dependability of Critical Information Infrastructures have therefore to be considered on a level, which goes beyond the local and national stakeholders to guarantee an acceptable level for economy, society, and politics.

Europe has recognised the challenges of Critical Information Infrastructure Protection (CIIP) with delay with respect to US, Canada and Australia. Long-term shared visions for research and exploitation among EU Member States as identified by EU Member States in the European Research Area (ERA) working group of the IST Committee (ISTC) and by various nations themselves are strongly needed.

Thus, the main objective of the **Critical Information Infrastructure Research Co-ordination** project is to create and co-ordinate a European taskforce to encourage a **co-ordinated Europe-wide approach** for research and development on Critical Information Infrastructure Protection (CIIP), and to establish a **European Research Area (ERA)** on CIIP as part of the larger Information Society Technologies (IST) Strategic Objective to integrate and strengthen the ERA on Dependability and Security.

In implementing an extended network of experts, expertise, and knowledge for CIIP, CI^{2}RCO starts from the hypothesis that national, regional and international research programmes with a wide variety of objectives do exist, which have direct or indirect relation to CIIP. Relevant players of research, research funding actors, policy makers and Critical Information Infrastructure stakeholders are mostly unaware of such CIIP related R&D programme similarities in various fields due to lack of knowledge, fragmentation, and limited networking capability, national need to know, restrictive policies and legal obstacles, as well as varying political structures across Europe. These factors lead to isolation and thus hinder an effectively netted and efficient research infrastructure in Europe.

CI^{2}RCO will therefore focus on R&D activities and actions across the EU-25 and Associate Candidate Countries (Bulgaria, Romania, and Turkey) that are essential to be carried out at European level and that require collaborative efforts involving research and research funding actors as well as other stakeholders across the European Research Area. This will be accomplished by the following set of activities:

1. Establishment of a CIIP-network of relevant players (as identified above)
2. Identification of completed, on-going and planned CIIP R&D programmes and projects on national and EU-level
3. Analysis of the European CIIP research area according to appropriate evaluation and assessment criteria
4. Calibration of the CIIP activities with CII stakeholders in a continuous feedback loop to identify gaps in the current and planned CIIP actions and activities
5. Elaboration of a European CIIP research agenda (roadmap) to determine R&D priorities
6. The organisation of workshops/conferences to initiate and to foster networks and to evaluate, to complete and to disseminate results
7. Provision of an Internet platform to supply sustainable support for information and co-operation of the CIIP-network.

After listening to the terms of references of the various initiatives, CI^{2}RCO feels it can contribute to and/or benefit from a number of initiatives, in particular:

- Security Research Initiative
- Internet Infrastructure Security Initiative

- Methods Standards Certification Initiative.

A2.10 Applications Security Initiative (ASI)

Presentor: Jim Clarke, Waterford Institute of Technology

The ASI is currently in the process of

- Taking stock and benchmarking current AS solutions
- Identifying dependencies with the others SI's
- Project impact of new security models on ASI
- Designing an ASI Rolling Roadmap.

The following organisations have registered within ASI:

1. Waterford IT
2. Telecom Italia Labs (TILABS)
3. Ethiqa SAS
4. University of Stuttgart
5. MarconiSelenia
6. Athens Technology Centre
7. Ericsson
8. Others TBC

The following Standards and other bodies are of relevance to the ASI:

a. IETF
b. W3C
c. European vendors of SSH, SSL
d. ETSI

The following gaps/challenges/bottlenecks have been identified in ASI for 2006-2010:-

- 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,)

The next steps for ASI can be described as:

1. Further Define Terms of Reference with the ASI team
2. Recruit new members/projects to ASI
3. Provide input to preliminary White paper following workshop
4. Draft the ASI document for comment (DFC)
5. Input to Call 5/Call 6/FP7/Beyond 2010)
6. ASI mailing list discussion (ASI@securitytaskforce.org with [ASI])
7. Produce the ASI DFC according to the schedule.

A2.11 "Securing open source infrastructures and applications, an methodological approach"

Presentor: Patrick Sinz, Ethiqa SAS

Just like any IT infrastructure, Free and Open Source Solutions (FOSS) needs to be secured, but it needs a specific focus. Free and Open Source solutions cannot be ignored, the technology and the economy around FOSS is here to stay.

Particularly in the Public Sector, FOSS is a critical component providing a way to improve:

- Transparency
- Sovereignty
- Ease of experimentation
- Open Sharing of knowledge

Particularly, the subsidiarity principle pushes responsibility and, therefore, the IT infrastructure toward regional authorities. This changes the way IT is deployed in the Public Sector and it also impacts who has to carry the responsibility for security and privacy. Obviously, the private sector has similar reasons to adopt Free and Open Source Solutions.

Security in Open Source used to be a minor concern for two very different reasons. On one side, most of the Open Source applications were not seen as “business critical”. On the other side, Open Source Infrastructure applications (mail, web server, routing, dns, ...) had been around long enough to be run under the gauntlet of various security attacks to be now quite secure. Moreover, with a development model that enables and encourage source code scrutiny, there is a general feeling that security issues are easier to spot and to solve by the community.

But with the wide adoption of Open Source solutions, the quantity of code to look at has grown significantly and the number of applications that are business critical has grown proportionally also. Moreover, new issues like Cross-Site Request Forgeries (CSRF) or (Cross-Site Scripting) XSS attacks are appearing at the application level. This leaves the FOSS world with issues of accountability and certification, and normalisation of architecture.

Trying to solve these using conventional processes will most probably not work, trying for instance to demonstrate that a specific firewall meets specific security requirements is not a trivial exercise. Therefore, the FOSS communities should adapt the process they already very successfully use to develop applications to also manage the security issues of their applications, and applications interactions/architectures. Much of the FOSS success is linked to the way FOSS infrastructures are built: what is commonly referred to as “FOSS relies on the collaboration of the Cathedral and the Bazaar to build a city”.

We needs to build a framework where the security needs of an Architecture can be modelled, defined, reviewed in an open and transparent manner, using the same “Forges” the application development already use. Basically defining a “contract model” between application elements, thus enabling not only the collaboration of application developers within a comprehensive framework but also the collaboration of service providers on a live application.

The goal is obviously not just to guarantee that an architecture « can » be secure, but that the specific way this architecture is run is secure.

A2.12 Internet Infra Security Initiative (IISI)

Presentor: Miguel Ponce de Leon, Waterford Institute of Technology

It is strange to say it, but the internet infrastructure we are looking to secure is contained in the little dot, of **.**com, **.**net and **.**eu. In this context, this initiative is looking at

the challenges of securing access to "User Centric Content" being transmitted across the internet.

User Centric Content for the work place is very much based on documentation cooperation, and online groupware systems, which facilitate teleworking, videoconferencing and real time negotiation.

For the personal space, User Centric Content is the communication of Infotainment, Blogs, and Online Albums.

This content is being communicated and exchanged across an Internet infrastructure, which is based on a web architecture, which is loosely coupled, transient in nature, and inherently insecure. The applications and services, which facilitate this exchange are becoming more distributed, using more machine-to-machine, and peer-to-peer paradigms, on a software middleware which has become increasingly complex (XML, Corba, J2EE, mobile agents).

Finally, the transmission media encapsulating this now incorporates both wired & wireless systems.

With these many variable factors in mind, the Internet Infrastructure Security Initiative (IISI) will look at:-

- Security models and technologies for the Internet as a whole.
- Advanced cryptography for multimedia content and eCommerce applications,
- Secure software middleware for the future Internet,
- Novel trust and security models for the Internet and interoperable ubiquitous computing environment,
- Internet home connectivity with the advent of ambient intelligent devices,
- Privacy, authentication, accounting and reliability for the Internet.

In researching these areas, IISI will have a number of challenges to address during 2006-2010:

- 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.

Having reviewed the workshop presentations on the day, the IISI research group will have a key strategic link with this WSI research group.

A2.13 "Corporate Perspectives on IT Security and Dependability"

Presentor: Dr. Tobias Christen, CTO Stonesoft

During the past 3-5 years, we observed significant shifts in how corporations invest into IT-Security. In the good old times, the network and application experts were seeing security as naturally important and asked for a security budget. Then IT budgets were browbeaten and all benefits had to be measurable and/or be a business enabler. At the same time, two pains were growing. On the one hand, protecting corporate resources (e.g. network bandwidth and working time) rose in importance and thus content filtering and bandwidth control were implemented to prevent, for example, P2P program usage, on the other hand virus/worm spreads culminated last year by shutting down corporate networks for hours and days. As a lesson learned, corporations started to implement better network segmentation with the possibility to quarantine sub networks (e.g. with blacklisting). Latest

at this stage, corporations started to think about security strategies that contained several levels of defense and made the granularity of protection more and more fine grained. Once you have established several layers of defense and made the protection fine granular, the amount of incident data starts to increase and requires a new level of manageability and automatic event correlation analysis.

Driven by major violations in corporate governance and subsequent severe bankruptcy of F500 companies, new laws were established to enforce good corporate governance. As a result, corporations restructured their risk-management and raised a risk-management scheme that looked at different type of risks in a structured and integrated way. Thus, also risk mitigation schemes (e.g. IT-Security protection measures and network & service availability) are integrated. The integration of these risks mitigation schemes can be achieved on many layers, however, the deeper the notions and concept unification goes, the more benefit a corporation can get out this integration. Integration on the highest level brings compliance to regulations. Going one layer deeper can already create better visibility and overview for the corporate risk situation. Going even further will facilitate the control and adaptation of corporate policies.

If a corporation wants to achieve a "fast time to market" for its e-business service, it is crucial that functional and non-functional requirements for security and dependability can be formulated from the very beginning. Applying security after the design of an application, or just testing for security after implementation of a business solution is not only slow but also inefficient. A fundamental aspect in quality assurance is that you need to be able to quantify the level of acceptance and to be able to do this for security you need to be able to formulate a risk-strategy that tells up to which level a risk is acceptable and when mitigation schemes need to be put in place. Even if risks are accepted, it is crucial to be able to detect whether such risk have realized, this again translates into better incident detection and incident management schemes.

Last, but not least, we observe that corporations are facing a significant challenge when increasing their e-business relationships. This increase can be caused for example by new ways of interacting with the supply chain but also because of new delivery channels to reach customers and solution partners. In effect this means that the current "on/off" type of security measures and trust relationships are no more 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.

A2.14 Identity and Privacy Initiative (IPI)

Presentor: StefanWeiss, Deloitte &Touche GmbH, for Prof. Dr. Kai Rannenberg, Goethe University Frankfurt.

Mr. Weiss presented a number of driving forces, activities and challenges involved in the areas of Identity and Privacy. These include the FIDIS NoE project, which stands for Future of Identity in the Information Society (www.fidis.net). FIDIS incorporates society, business and technology Views and is in close cooperation with the IP PRIME project. FIDIS is bringing together a heterogeneous collection of initiatives.

The Integrated project PRIME, which stands for Privacy and Identity for Europe (www.prime-project.eu.org) is engaged in research on PET, Privacy Management (PM) and integration of PM into IM.

There are a number of joint research activities between these two projects including Identity Management definition (status, taxonomy), Profiling, Interoperability of IDs and ID management systems, Forensic Implications, De-Identification, The HighTechID and Mobility and Identity.

Mr. Weiss presented some of the motivational factors for Identity Management, which include usability, control (Audit Issues), efficiency and privacy.

Areas of problem areas for further research include compatibility (Standards), increasing laws and regulations (enforcement, forensics), societal changes (privacy behaviour) amd new identity and privacy issues within mobile applications

In conclusion, 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).

The following organisations have registered within IPI:

- Goethe University Frankfurt Deloitte & Touche GmbH
- SETCCE
- Independent Centre for Privacy Protection Schleswig-Holstein, Germany
- UNI Stuttgart
- University of Applied Sciences of Bern
- LAKE Communications.

A2.15 Biometrics Security Initiative (BSI)

Presentor: Orestes Sánchez Benavente, Telefonica I+D

The presentation started with a description of initial results on the mass deployment of biometric systems and the challenges that need to be addressed for the the integration of biometrics in every-day scenarios, which includes robustness and trust.

A number of user-based concerns were described on the deployment of security technologies in an open and proactive environment like that of the Ambient Intelligence Space. The Ambient Intelligence Space is a seamless, ubiquituous and computer populated environment that reacts to the user. The concerns include data protection, privacy, security perception, usability, acceptance, convenience, discussion with users and citizens and scenario development.

A number of other environments were described in which Biometrics could be prevalent such as mobile and nomadic applications in which there are more and more open environments, electronic transactions such as eGovernment, eCommerce and mCommerce and other large-scale deployments.

The standards bodies of relevance were presented. These include:-

- ISO JTC1 ISO SC37
  - §BioSec and BioSecure applied for Category A liaison
  - §European participation in the committee
- CEN/ISSS Focus Group on Biometrics
  - §BioSec is participant
- EBF Standardisation working group
  - §SAGEM is leading the WG
  - §Telefonica is participating

The following projects have elements that pertain to the BMI:-

- BioSec (IP). End by Nov 2005
  - §Biometrics and security through all the elements of the auth chain
  - §Aliveness detection, robustness, usability, performance eval
- BioSecure (NoE). End by June 2007

§Biometrics for secure authentication
§Multimodality and performance evaluation

- SECURE-Justice (STREP). End by Feb 2007
  §secure communication and collaboration framework for the judicial co-operation environment
- Digital Passport (STREP). 36 months
  §Digital passport and PKI
- SecurePhone (STREP). 30 months
  §Secure contracts signed by telephone
- Telefónica I+D (Spain)
  §BioSec project coordinator
- ATOS Origin (Spain)
  §SecurePhone project
- SAGEM (France)
- International Biometric Group (UK)
- @bc consulting (Germany)
- Robotiker-Tecnalia (Spain)
  §SecurePhone project

New members are welcomed and invited to join the BMI at www.securitytaskforce.org.

The key challenges facing the BMI were presented. They include User-centred challenges including the legal framework, identification of acceptance barriers, cross-European studies and education. There are a number of technical challenges including multimodal biometrics, aliveness detection, robustness, secure Storage, and network authentication. There are a number of certification issues including evaluation of performance, interoperability and security. There is an challenge related to overall coordination and leadership in the field including Standardisation. There are also a large number of challenges relating to Applications using biometrics including verification of identity in new areas like e-Government, e-Health, e-Everything, scenarios for Ambient Intelligent Space, dealing with networked applications, every-day applications with requirement for private identification, biometrics in electronic signatures, biometric encryption, ROI and cost estimation, and large scale deployments.

The presentation concluded with a description of the next steps for the BMI. These include invitation of stakeholders from industry, academia and policy makers to contribute, build liaison with other initiatives, build scenarios with a top down approach, aggregate list of research challenges using a bottom-up approach and determine how best to fill the gaps and finally to suggest coordinated actions in the areas of standardisation and the legal framework.

A2.16 Security Architecture and virtual Paradigms Initiative (SVPI)

Presentor: Atta Badii, School of Systems Engineering, Computer Science Dept., University of Reading

The SVPI Terms of Reference is **e**xploring 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 communicating domains and their enclosures to allow S&T services selection, composition and matchmaking. 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 (e.g. Badii & Tilo-Balke 2002).

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.

The above challenges, in the context of ambient intelligence and the increasing use of mobile devices with limited resources, demand an entirely new breed of on-device scalable and adaptive middleware to hide the complexity of maintaining secure communications management from the applications layer.

From a systemic and responsibility-theoretic viewpoint, the pre-requisites for provisioning a range of security systems and services at component and systems level include some of the following systemic properties as appropriate:

- Socially acceptable, routinise-ability and graceful integration into legacy and real-time embedded systems
- Semantic Integrity, Inter-operability, Integration and Continuity – semantic I^3C statefulness
- Self-monitoring and performance measurement within a universal Testability Framework
- Context-awareness and situation assessment, knowledge reporting and enquiring as necessary
- Learning capable, re-adaptive, layered, scalable, modular, resilient, reconfigurable, re-purposable
- Invocable flexibly (including stage-able incrementally as needed, multi-path, parallel algorithm implementation).

In terms of SVPI for dynamic S&T protection services, this indicates the following research issues:

1. Distinguishing virtual communication domains across whose boundaries scalable security services could be tasked to manage a user's dynamic S&T chain in the context of user's business logic and value chain. Thus for each such client device/user three

interacting domains are virtualised to include all hardware and software modelled under each of :

- Self-Domain (S): All HW/SW constituting user's personal client devices (home computer, office computer, laptop, PDA, mobile phone and native applications running on them (calendar, diaries, profilers etc).
- Others-Domain(O), All HW/SW belonging to all other parties transacting with the user including that of peers and grid-enabled services.
- Smart-Middleware-Domain(M): Any component involved in mediating data exchange across the boundaries between the above two domains.

2. Establishing a universal standard taxonomy of security contexts and boundaries through robust and senseful context descriptors.
3. Remote device interrogation re device-id, profiles, protocols capability, S &T rating
4. Recognition of content, device, location (physical, network-topological, distance), context, and context switches.
5. Implementation of self-monitoring, and self-state-aware, link-state-aware, context-aware nodes.
6. Universal device security status language for security dialogue and updates between smart-secure middleware communication managers.
7. Generalisation ontologies for relating one context to another and reasoning over context switches across time, place and space.
8. A security sensor and data intelligence network including security screening units at major trunks upstream of network and beyond enterprise domain boundaries as well as at nodes/gateways within the enterprise to allow security assessment and local-global security knowledge updates.
9. Secure global time-&-counts stamping to support secure access & DRM (e.g. recording, stamping and verification of licensing/certifications dates, or number of times an item (say play licence) is used, or a certificate has been renewed, etc.
10. Enhanced mutual security cooperation model.
11. Distributed security management within a regulated security environment with universal ID/key management, security metrics and domain security/vulnerability ratings, DRM and security escalation rules; heterogeneous security protocols, heterogeneous and dynamic network topologies, dynamic agent roles/structure/interaction patterns.
12. Semantically recompose-able sets of distributed security services optimised Call-by-Call.
13. Global malware id-system, multi-view correlation and visualisation of attack patterns and contagion mapping (dynamic attacks cartography) to aid attack prediction and knowledge management by reference authorities to accelerate security protection and recovery from attacks.
14. The architectural implication for the possible requirement at each point in the S&T chain each layer to be capable of:
    - S&T threat scenario situation assessment
    - S&T threat scenario pre-emption & threat chain breaking
    - S&T threat scenario forecasting, simulation, socially intelligent fixes & failure recovery policies enactment
    - S&T threat pre-emption eco-system (immuno-genetic modelling) to combat the attackers' eco-system i.e. match the attacker's re-learn-re-innovate-re-attack chain so as to enable enhanced pre-emption, prevention and recovery in a dynamic attack environment.

15. The extent to which a new framework of secure programming models and secure hardware design should be established as a set of best practice guidelines to encourage and accelerate the scalable design of security properties in components as appropriate.

A2.17 Methods, Standards and Certification Initiative (MSc I)

Presentor: Alan Husselbee, Information Systems security association (ISSA).

The presentation aimed at building awareness of the Standards community to the Security task Force participants (Reference Framework and context), current difficulties (Challenges), ways to move forward (anticipated actions of MscI) and the possible outcome (Expected results).

The probable result of the MSc Initiative would be to initiate actions leading to the measurable improvement of training and certification in security standards of European companies, products and personnel. The current certification process has a very American orientation and is not within ISO whereas the tendency is towards certification in ISO security standards that have a European orientation (ISO 17799 for example).

The global framework governing the security industry standards development was shown with reference to the diverse organisations such as W3C, IETF, The Open Group, etc., and special mention was made of the COPRAS project in the 6th Framework which is helping the other framework projects to correctly align themselves with the European standards effort, so that they can make worthwhile contributions. It is significant that the COPRAS project exists. The need for the COPRAS project underlines the current lack of understanding and awareness on the significance of standards not just within the R&D Framework community, but also generally. This is why it is difficult to pinpoint other projects having an interest in MScI. All current interest (as happens also in standards) is by individuals and by the standards organisations themselves (CEN/ISSS workshops).

The changing paradigm on current challenges to the Security community 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 major concern is “Is the standards development process able to change and respond to the new paradigm?” Present day difficulties are numerous, however. Among them is the extremely long time (2 to 5 years) it takes to develop a consensus on a standard within the ISO world. One solution is the current fast track approach (6 to 12 months) recently used for ISO 17799. Another solution is the approach used by IETF (Request For Comment RFC) which can take just 3 to 6 months and is low cost (via internet work groups). Another issue is the lack of participation from the user community. Yet another is the relative high cost for an SME to send a member of staff to participate in the international for a.

One major difficulty is that security issues are the concern of all the standards organisations and visibility on the issues being worked upon is not always available. It is here that the Security task force can make a major contribution to improving liaison between the different groups.

Among the tasks that could be taken on board by MscI are :-

- Producing a mapping of security standards in line with the SC27 proposed model framework so that any anticipated standards work can refer to the map to establish possible liaisons.

- Produce a mapping of the current and proposed interoperability of the different standards organisations on security
- Produce a schematic capability maturity Model for R&D 6th Framework actions in security standards
- Make recommendations for improving user and SME participation in the security standards process and security standards implementation
- Make recommendations for improving the reactivity of the European initiatives on issues and resolving them (such as increasing the funding available for rapid & necessary actions from expert groups)

The above actions will help with the redevelopment of the overall security policy and strategy for 2007 to 2013.

A2.18 Cryptography Research Initiative

Presentor: Prof. Bart Preneel, K.U.Leuven (Belgium)

The presentation started with the observation that even if cryptology is now "widely used" (TLS, IPsec, GSM, Bluetooth), the cryptology problem is not solved for the long-term. Cryptographic schemes always offer a trade-off between security, performance and cost (footprint, power consumption). It is not too difficult to achieve one of these three properties at the expense of the other two. However, in my applications, one needs two or even three properties. This clarifies the need for improved designs, particularly because the threat model and environment is changing

- When we evolve to an *ambient intelligent world*, privacy concerns will increase and cryptology will need to be everywhere (even in the smallest devices). This means that 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.
- For *highly sensitive applications*, (e.g., medical data) there is a need for cryptographic techniques that can offer very high and long-term security (50 to 100 years) at a reasonable performance and cost. For these applications, one needs to take into account that existing schemes (particularly public key cryptology) may succumb to progress in mathematics (number theoric progress such as novel factoring algorithms) or progress in computation (large quantum computers may be built in the next 15 to 20 years which are able to break schemes such as RSA, and (hyper-)elliptic curve cryptography).
- For *high end applications*, there will be a need for cryptographic techniques that can offer extreme performance at a reasonable cost. This trend will become more important since the storage capacity and communication speeds grow much faster than computational power. Hence, where today encrypting a hard disk or a communication line represents a limited overhead, this will change in the future. Optical cryptology may be needed to keep up.
- The protection of *media* introduces the need for advanced techniques for watermarking and perceptual hashing. In this area there is also a strong need for better models and definitions.

Even in the current environment, we have witnessed in the last years a large number of new attacks on hash functions (MD4, MD5, SHA and even SHA-1) and on a broad class of stream ciphers. Hence, there is a clear need for new designs that can replace the current solutions in the next years.

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). Overall, there is a very strong need to expand and strengthen an approach that takes into account rigorous models and provable security.

Annex 3. Workshop Agenda

Date: April 19th 2005, held at Centre de Conférences Albert Borschette (CCAB), Brussels

Session 1. Opening Session

09h30 – 10h00 Introduction
Session Chair - Dr. Willie Donnelly, Waterford Institute of Technology
Welcome Address: European Strategic agenda on Security and Dependability
Andrea Servida, European Commission

Session 2. Security Task Force Initiatives

10h00 – 13h00 Introduction
Session Chair – Jim Clarke, Waterford Institute of Technology
Dependability and Trust Initiative (DTI)
Prof. Brian Randell, University of Newcastle Upon Tyne, for Prof. Paulo Verissimo, FCUL
"Context-aware Security and Trust"
Guest Speaker: Konrad Wrona, SAP Labs France
Security Policy Initiative (PCI)
Prof. Antonio Lioy, Politecnico di Torino
"Toward a culture of security in Europe"
Guest Speaker: Dr. Ronald de Bruin, European Network and Information Security Agency (ENISA)
Cryptography Research Initiative (CRI)
Prof. Bart Preneel, Katholieke Universiteit Leuven
Wireless Security Initiative (WSI)
Bosco Eduardo Fernandes, Siemens
"Wireless Device Id in the Ambient World - From Identification to Context Adaptable Recognition"
Guest speaker: Stephan Engberg, Open Business Innovation
"SecurePhone project"
Guest speaker: Erik Nørgaard, Atos Origin
Security Research Initiative (SRI)
Dr. Sathya Rao, Telscom.
"Critical Information Infrastructure Protection"
Guest Speaker: Uwe Bendisch, Fraunhofer Institute for Secure Information Technology (SIT) Department

13h00 – 14h00 Lunch

14h00 – 16h30 Internet Infra Security Initiative (IISI)
Miguel Ponce de Leon, Waterford Institute of Technology
"Corporate Perspectives on IT Security and Dependability"
Guest Speaker: Dr. Tobias Christen, CTO Stonesoft
Identity and Privacy Initiative (IPI)
StefanWeiss, Deloitte &Touche GmbH, for Prof. Dr. Kai Rannenberg, Goethe University Frankfurt.
Biometrics Security Initiative (BSI)
Orestes Sánchez Benavente, Telefonica I+D
Security Architecture and virtual Paradigms Initiative (SVPI)
Prof. Atta Badii, University of Reading
Applications Security Initiative (ASI)
Jim Clarke, Waterford Institute of Technology
"Securing open source infrastructures and applications, an methodological approach"
Patrick Sinz, Ethiqa SAS
Methods Standards Certification Initiative (MScI)
Alan Husselbee, ISSA

Session 3. Setting security priorities (2006-2010)

16h30 – 17h00 Outline of Roadmap – next steps
Session Chair – Dr. Sathya Rao, Telscom
Closing Remarks
Dr. Willie Donnelly, Waterford Institute of Technology

Annex 4. List of Participants

Henning Arendt	@bc
Omid Aval	Smarticware AB
Atta Badii	University of Reading
Uwe Bendisch	Fraunhofer Institute for Secure Information Technology
Jerome Billion	Trialog
Karima Boudaoud	Laboratoire I3S-CNRS
Tobias Christen	Stonesoft
Jim Clarke	Waterford Institute of Technology
Bruno Crispo	Vrije Univeristeit Amsterdam
Ronald De-Bruin	ENISA - European Network and Information Security Agency
Willie Donnelly	Waterford Institute of Technology
Andrea Servida	European Commission
Sofoklis Efremidis	INTRACOM S.A.
Stephan Engberg	Obivision
Alain Esterle	Central Directorate for Information Systems Security
Bosco Eduardo Fernandes	Siemens
Anestis Filopoulos	Digitalis Consult
Ulrich Friedrich	Atmel
Antonio F. Gómez Skarmeta	Universidad de Murcia - Spain
Alfred Gottwald	Siemens
Thomas Haeberlen	ENISA - European Network and Information Security Agency
Ulf Hägglund	Smarticware AB
Jarkko Holappa	VTT Electronics
Alan HUSSELBEE	ISSA
David-Olivier Jaquet-Chiffelle	University of Applied Sciences of Bern
Jörg Kaiser	University of Ulm
Peter Kirstein	University College London
Henry Kraseman	Independent Centre for Privacy Protection Schleswig-Holstein
Michael Kreutzer	Darmstadt University of Technology
Latif Ladid	Independent Consultant
Gerardo Lamastra	Telecom Italia - TILAB
Antonio Lioy	Politecnico di Torino
Javier Lopez	UNIVERSITY OF MALAGA
Fulvio Marcoz	Finmeccanica
Evangelos Markatos	FORTH (Foundation for Research and Technology - Hellas)
Sadhbh McCarthy	Local Government Computer Services Board
Alexandra Michy	SAGEM
Christian Monyk	ARC Seibersdorf research - Austria
Erik Nørgaard,	Atos Origin
Brian Randell	University of Newcastle upon Tyne
Sathya Rao	Telscom Consulting
Mark Reilly	Enterprise Ireland
Silvia Renteria	ROBOTIKER-TECNALIA
Orestes Sanchez-Benavente	Telefonica I+D
Reijo Savola	VTT Technical Research Centre of Finland
Tom Sheedy	Enterprise Ireland
Luca Simoncini	Department of Information Engineering- University of Pisa

Patrick Sinz	Ethiqa SAS
Luc Van den Berghe	CENORM
Ines Vidal	Euskaltel, S.A.
Kush Wadhwa	International Biometric Group (UK)
Jan Weber	Omega Management Consultants
Stefan Weiss	Deloitte & Touche GmbH
Tim Willoughby	Local Government Computer Services Board
Konrad Wrona	SAP Labs France
Miguel Ponce de Leon	Waterford Institute of Technology
Fabio Ghioni	Telecom Italia
Carston Rust	R&D Smart Cards
Andre Cotton	Thales Communications
Thomas Engel	Université du Luxembourg
Anestis Filopoulos	Digitalis Consult
Anna Plataki	Infineon Technologies
Neeraj Suri	TU Darmstadt, Dept. of Computer Science
Maria Karaguiozova	Infineon Technologies
Tom McCutcheon	Dstl
Mathieu Gorge	VigiTrust
Simin Nadjm-Tehrani	Linköping University
Christian Tafani	Institut du Droit de la Paix et du Développement (IDPD)
Prof. Bart Preneel	Katholieke Universiteit Leuven
Francois Armand	Jaluna
Don Villa	Euroclear
Brian Randell	University of Newcastle upon Tyne
Christian Kollmitzer	ARC Seibersdorf research GmbH
Manuela Stimpfl	ARC Seibersdorf research GmbH
Marc Idelson	ISSA
Bernhard Hämmerli	Acris GmbH und HTA Lucerne University of Applied Science
Selçuk Taral	TÜBITAK-UEKAE
Kostas Zygouraitis	Intracom
Karima Boudaoud	ESSI