SecurIST: Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D

by James J. Clarke and William M. Fitzgerald, *Telecommunications Software & Systems Group (TSSG), Waterford Institute Of Technology Ireland*
jclarke@tssg.org, wfitzgerald@tssg.org

Abstract

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

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

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

This paper provides a brief overview of SecurIST and an introduction to the Security Task Force Initiatives that have been formed. Companies and projects wishing to join these initiatives can still register their interests at **www.securitytaskforce.org.**

Introduction

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

The research agenda must

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

Organizational Structure

As shown in Figure 1, the project approach is to create consensus among the key European industry and academic players on the security and dependability research priorities for FP6. The approach is to build on what has already been achieved through the Framework 6 security workplan.

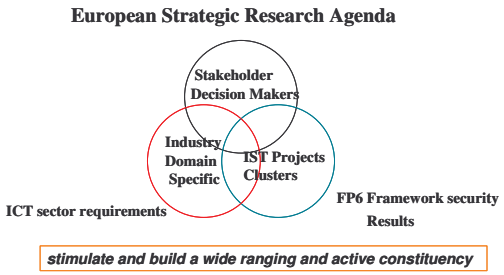

Figure 1. Org. structure

This focussed effort will be achieved through:

- **Creation of a security taskforce**

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

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

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

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

- **Establishment and management of the Security Advisory Board.**

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

Security Task Force Initiatives

The following areas of security and dependability research today have been identified and the following Initiatives were established following two successful Workshops held in Brussels during January and April 2005 under the umbrella of the Security and Dependability Task Force [1].

Dependability and Trust Initiative (DTI)

DTI is concerned with two main issues: the confluence between classical dependability and security, met essentially but not only by the concept of common 'accidental fault and malicious intrusion tolerance'; and the necessary but often forgotten link between trust (dependence or belief on some system's properties) and trustworthiness (the merit of that system to be trusted, the degree to which it meets those properties, or its dependability).

The objectives of DTI are centred on two main axes:

1. To foster the development of techniques, methodologies and architectures that take into account the common goal of achieving resilience to accidental and malicious faults;
2. To stimulate awareness about the need to build systems that are simultaneously secure and dependable, in the user and technology researchers and developers communities.

Security Policy Initiative (SPI)

The ICT systems have become so complex that it is nearly impossible to design and manage their security in a global and reliable way. We envision to use a formal policy as the foundation to create computer-assisted security design and management system to support managers in the difficult task of defining and implementing a desired protection policy. Given an adequately high and general level of the policy, this should let managers

concentrate on high-level rules rather than implementation details (that could be automatically derived by appropriate tools). Moreover, a high-level policy would also be beneficial for auditors by providing them with a formal specification to check compliance with user requirements and measure actual achievements.
One objective of SPI is to survey the state of the different existing efforts related to policies and policy-based management, with special interest into all those efforts (and there are not many) specifically related to security. Another objective is to identify areas needing further research to fulfil the vision of a future multi-vendor, multi-level, policy-based security management system.

Wireless Security Initiative (WSI)

WSI targets security in Mobile/ Wireless service environments. It will address Ambient Radio, Ambient Networks and User Device capabilities in a 3G/3G beyond environments, 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.

Some of the main items to focus on are:

- 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).
- 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.
- Regulatory aspects especially in regards to: Lawful interception, Anti-fraud policy, Regional policy,
- Secure neighbour discovery, especially in regards to: MIPv6 and AAA integration, Interdomain issues and Key management.
- Security in sensor and ad hoc networks.
- Research in Access and Smart Cards/USIM/ISIM very important and need further investigation.
- Ambient intelligence security.
- 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.

Security Research Initiative (SRI)

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

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.

The objectives of ASI are to benchmark current application level security programs and develop a strategy to build improved application level security programs in the future based on past and current best practices. To achieve this, the ASI initiative must also draw on the knowledge of other security initiatives within the security taskforce forum.

Internet Infrastructure Security Initiative (IISI)

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.

The IISI team have a number of objectives to achieve such as standardising new security models and technologies for the internet as a whole. Novel trust and interoperable security models for the internet in ubiquitous environments will be addressed. Also privacy, authentication, accounting and quality of service (QoS) for the internet will be researched.

Identity & Privacy Initiative (IPI)

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

The objectives of IPI are to monitor the ongoing research in the field of identity and privacy and to collect further research topics, especially suitable for elaboration in FP7. These topics focus mainly on technological research and development, but - as the field is highly interdisciplinary - also comprise issues and approaches of other disciplines, e.g., law, economics, sociology, psychology, and usability. The initiative contributes to standardization in this developing field.

Biometrics Security Initiative (BSI)

BSI is addressing 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. BSI interests also includes: new algorithms, alternative solutions, novel pattern recognition approaches, multi-modal biometrics, data fusion issues, standardization of testing bio data and so forth.

BSI objective is promoting the use of biometrics in ICT scenarios that would solve society problems and would serve as an initial platform for the deployment of advance, cost-efficient and secure identification systems.

Security Architecture and Virtual Paradigms Initiative (SVPI)

SVPI is exploring socially intelligent architectures for best value ubiquitous management of the dynamic Security & Trust (S&T) chain across time, place and space; end-to-end. This research area involves architecting the semantic representation of distinct communicating domains and their enclosures (boundaries, sub-systems) so as to facilitate S&T services selection, composition and in general dynamic context-dependent S&T matchmaking for adequate security protection of each interacting domain and entity.

This entails providing adaptive and personalised protection for each entity through distributed management and delegation of security protection to smart grid-enabled proxy services. Such security services should be invocable ubiquitously when required on a Call-by-Call security services outsourcing basis.

1.10.2 Objectives of SVPI

From a systemic and responsibility-theoretic viewpoint, the pre-requisite framework 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, reutilise-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.

- Invocable flexibly (including stage-able incrementally as needed, multi-path, parallel algorithm implementation).

Methods Standards Certification Initiative (MScI)

The MSc Initiative 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:-

1. A measurable improvement of the number of participants in security standards workshops and standards organisations across Europe, especially from the New Member States, and
2. an increase in the number of European companies, products and personnel obtaining certification in security standards
3. Improvement of the existing security standards methodology and process in order to drastically reduce the time to market for the development of security standards.
4. Proposed actions could take the form of R&D security projects within the 7th Framework programme.

Cryptology Initiative (CRI)

CRI is focusing on advanced and novel cryptographic algorithms and protocols and on techniques for watermarking and perceptual hashing. The emphasis is on a close cooperation between theory and practice, with sufficient emphasis on theoretical foundations but also on implementation issues.

The goals are to improve security and confidence in cryptographic techniques, also for the long term, and to develop secure and efficient implementations and finally to integrate these techniques into advanced applications such as electronic voting, fighting spam, digital asset management and privacy enhancing technologies. At the technical level, this translates into improved trade-offs (security/cost/performance) for cryptographic algorithms and better design and analysis techniques for complex protocols.

It is also very important to reduce the gap between advanced research in cryptology and the cryptology applied in real-life applications both in terms of more up to date and future-proof algorithms and in terms of protocols for distributed trust. Better coordination of standardization in this area (both national and international)

Advanced cryptographic techniques need to be developed for specific applications 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), and privacy (efficient mixes and credentials).

Finally there is a strong need for advanced techniques for watermarking and perceptual hashing, both from a theoretical point of view (definitions, models) and from a practical point of view.

Conclusions

This paper only has room to cover an overview of the SecurIST project and the STF Initiatives and their terms of references. In order to find out more about the valuable work in progress in determining the key challenges being faced within these thematic areas, we invite you to participate further in the STF by registering at www.securitytaskforce.org.

References

[1] Clarke, et. al., **STF-DFC01_Final,** Security and Dependability TaskForce (STF) Document for Comments (DFC), July 2005.

Acknowledgement

SecurIST (FP6-004547) is a project funded by the European Commission's Sixth Framework Information Society Technologies (IST) Programme, within the Unit ICT for Trust and Security.