Journal of Computer Security 18 (2010) 1–5
DOI 10.3233/JCS-2010-0375
IOS Press

Introduction

JCS special issue on EU-funded ICT research on Trust and Security

Jan Camenisch [b], Javier Lopez [c], Fabio Massacci [d], Massimo Ciscato [e] and Thomas Skordas [e,*]

Members of the Editorial Committee of the special issue

[b] *IBM Zurich Research Laboratory, Zürich, Switzerland*
[c] *University of Malaga, Malaga, Spain*
[d] *University of Trento, Trento, Italy*
[e] *European Commission, DG INFSO Unit F5 "Trust and Security"*

Security and trust are core research issues for the further development of the Information Society and for 10 years have played, and continue to play, an integral part in the European Union's Framework Programmes (FPs) for R&D.

EU-supported collaborative research projects in trust and security bring together multi-partner stakeholders from industry (technology and service providers, system integrators and end-users), academic and research laboratories working in several interdisciplinary research fields. Sometimes, projects include actors from the legal, social and economic sectors. Together their joint efforts permit a better understanding of the conflicts and synergies between security, privacy and free market economics, as well as of the psychology and sociology of trust and security when building and deploying new technologies. The long term goal for funding this research effort is to convert the know-how of the EU in security, privacy and trust into economic advantages.

In the period 1998–2002, under FP5, original and ground-breaking scientific & technological (S&T) work took place in ICT Trust and Security. Key S&T developments achieved at that period included significant advances in cryptology, smart cards and biometrics. EU-supported research also permitted the identification of new concepts in fields of work such as privacy, dependability and risk analysis.

In the period 2002–2006, under FP6, research efforts in ICT security and trust have been further intensified. As part of the FP6-IST Programme, 37 R&D projects

*Corresponding author: Thomas Skordas, European Commission, BU25-5/94, B-1049 Brussels, Belgium. Tel.: +32 2 29 68 908; Fax: +32 2 29 68 364; E-mail: Thomas.Skordas@ec.europa.eu.

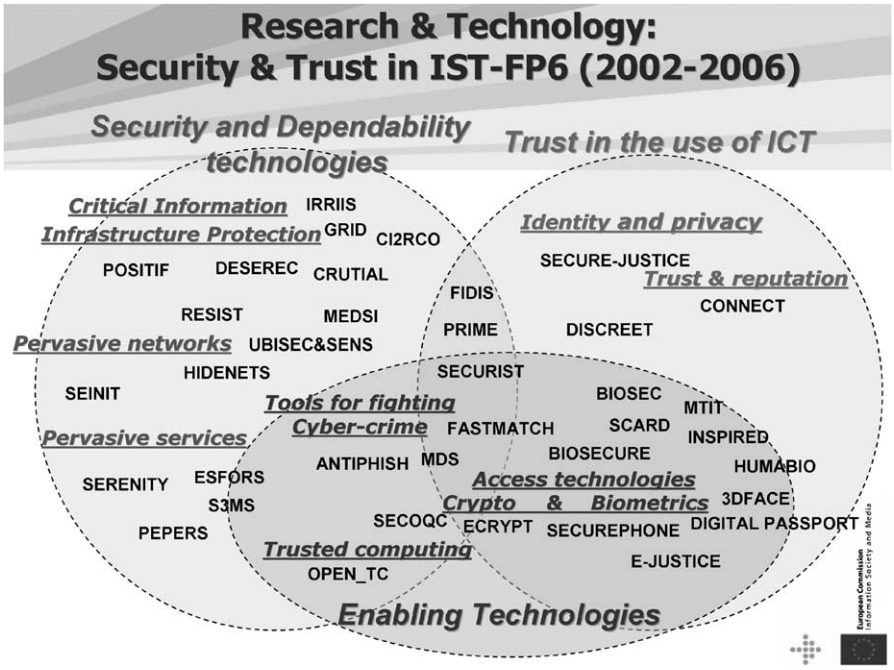

Fig. 1. Project portfolio in the area of Trust and Security under FP6-IST: 37 R&D projects receiving a total of €146 million EU funding.

have been funded, with a total value of around €245 million (circa €146 million funding from the European Commission). Figure 1 clusters these 37 projects around the following three main themes:

- *Security and dependability technologies* including: new security and dependability architectures that are resilient to system failures or cyber-attacks; scalable and interoperable security policies; secure and dependable mobile applications; understanding, managing and controlling the interdependencies of critical infrastructures; and platforms for secure service composition and provisioning.
- *Technologies for privacy and trust* cover: end-to-end security in data communications and storage; novel, interoperable identity management systems that are privacy respecting and empower the users to manage their own credentials; and, technologies that ensure the protection of personal data and privacy and properly assign liability and risks, together with the appropriate governance models needed to do so.
- *Enabling technologies for ICT security and trust* such as: network traffic monitoring for detecting and dealing with spam, phishing and other malware; interoperable and open trusted computing platforms; new cryptographic schemes coping with very high data transfer rates or with scarce computing and power

resources; advanced multi-modal biometrics; and technologies for assessing the trustworthiness of ICT infrastructures and services.

The majority of the 37 projects have been completed, and the remainder are due to deliver their final results soon. Further information concerning these projects may be found at: http://cordis.europa.eu/ist/trust-security/index.html.

In the period 2007–2013, under FP7, research on trust and security continues to be one of the core research fields supported by the EU. Within 2008, 33 new research projects were launched. Further information on the newly launched EU-funded projects in this field is available at: http://cordis.europa.eu/fp7/ict/security/home_en.html.

For this special issue of the Journal of Computer Security (JCS), FP6-IST research projects that were still ongoing at the time of the call for papers and that received outstanding reviews have been invited to submit their scientific research results. From the 16 invited projects that submitted papers, six of them were finally accepted through the standard JCS peer review process and are presented in this special issue. In the remainder of this introduction, these papers are briefly presented:

Paper "New filtering approaches for phishing email", by the IST project ANTIPHISH (http://www.antiphishresearch.org/). Today's state-of-the-art anti-phishing approaches are not broadly implemented. They lack completion or require a high administrative overhead. In this paper, ANTIPHISH Partners present some new and effective solutions addressing e-mail phishing. They concentrate on countermeasures based on the contents of phishing e-mails and describe a number of novel features that are particularly well-suited to identify phishing e-mails. The range of proposed features include: statistical models for the descriptions of e-mail topics, sequential analysis of e-mail texts and external links contained in an e-mail, detection of embedded logos, and indicators for intentional addition or distortion of content not perceivable by the reader. The new solutions have been tested using a large real-life corpus of e-mails pre-labelled as spam, phishing, and legitimate. The results for the classifications of phishing versus legitimate and phishing versus legitimate and spam indicate that the authors achieve very low error rates and outperform other schemes previously proposed for classifying phishing e-mails.

Paper "Provably correct inline monitoring for multithreaded java-like programs", by the IST project *S3MS* (http://www.s3ms.org/index.jsp). Today's mobile devices have the computing power to offer users many more applications than currently available. *S3MS* developed the 'security-by-contract' paradigm, which essentially consists of the use of policies, monitoring, and monitor *inlining* to secure third-party mistrusted applications running on mobile devices. Inlining is a program rewriting technique to ensure that a program complies with a given security policy. The paper presents the design and implementation of inlined reference monitors. More precisely, a security state is embedded into the client program and code rewriting is used in order to ensure that such a state is queried and updated appropriately. This solution presents some very original features: firstly, it allows for automatic enforcement of a previously defined policy; and secondly, since the policy is formulated in

a 'contract' (i.e., a piece of code) that accompanies the program, the policy is easily available for consultation to interested parties.

Paper "Security of trusted repeater quantum key distribution networks", by the IST project *SECOQC* (http://www.secoqc.net/). Modern cryptography relies on the use of digital 'keys' to encrypt data before sending it over a network, and to decrypt it at the other end. The receiver must have a version of the key code used by the sender so as to be able to decrypt and access the data. Quantum key distribution (QKD) offers a theoretically uncrackable code, one that is easily distributed and works in a transparent manner. Even better, the nature of quantum mechanics means that if any eavesdropper tries to snoop on a message, the sender and receiver will both know. The *SECOQC* project has investigated the feasibility of an open QKD infrastructure, together with the enabling technology. The aim was to enhance the existing landscape of security technologies with novel and reliably secure ways of performing long-range and high-rate distribution of secret keys. The paper proposes a provably secure method using the QKD protocols in a trusted key repeater network. The deployment of such a network is feasible with current technology (ordinary computers and optical networks) and will most likely be the way quantum key-distribution will be employed in the real world.

Paper "Towards automated security policy enforcement in multi-tenant virtual data centers", by the IST project OPENTC (http://www.opentc.net/). Securing our computing systems and making them trustworthy is one of the most challenging problems in computer science for the years to come. The OPENTC project aimed to improve the security of computing infrastructures by combining virtualization and trusted computing using open-source software. Virtual systems allow for fine-grained isolation of confine attacks as well as errors. Trusted computing enables stakeholders to validate the configuration of given systems. The use of open source components allows users to examine, validate, and improve upon the functionality of the trusted computing base. Exemplifying that at a specific scenario, the paper presents a security architecture for virtual data centres based on Trusted Computing technologies. The architecture allows for the automatic deployment of the security mechanisms required by the policy that was specified for the particular service. The authors have shown the viability of their approach by a reference implementation.

Paper "Exploiting cryptography for privacy-enhanced access control", by the IST project *PRIME* (https://www.prime-project.eu/). *PRIME* has targeted solutions to enable Internet users to manage their digital identities according to their specific circumstances and to support providers in handling personal data in ways that respect the privacy of users. The project developed privacy-enhancing mechanisms and integrated them into a working prototype of a privacy-enhancing identity management system. The paper targets the issue of privacy policy languages that use high-level cryptographic primitives. The core idea of the paper is that, although a number of privacy enhancing cryptographic primitives have been proposed in the literature, these have mainly been focussed on the cryptographic details. As a result, using anonymous credentials for privacy protection in a real-life scenario is difficult for anyone

other than a cryptographer. In this paper, the authors present the cryptographic constructions for anonymous credentials, and the relative extensions needed for practical applications. They then describe a high-level policy language that enables system designers to take advantage of those cryptographic mechanisms to protect the privacy of users. With respect to the development of privacy-enhanced systems, such policy language might play a similar role to the one that high-level programming languages have played with respect to machine languages.

Paper "Biometric template protection in multimodal authentication systems based on error correcting codes", by the IST project *HUMABIO* (www.humabio-eu.org). *HUMABIO* was concerned with human monitoring and authentication using biodynamic indicators and behavioural analysis. Biometric authentication, particularly at airports, is one of the most widespread and visible security mechanisms. The paper demonstrates an advanced stride forward in establishing and improving such authentication mechanisms. It proposes a framework for authentication combining data from multiple biometric sensors, e.g., facial and gait properties. The proposed solution not only improves the identification process, but also protects the privacy of users by hiding their original templates using cryptography. The underlying idea is to consider the biometric recognition as a distributed source-coding problem to which well-known error correcting codes can be applied. The authors have shown the viability of their system with tests at an airport.

Acknowledgements

The Editorial Committee members and the European Commission's DG INFSO Unit "Trust and Security" would like to warmly thank the reviewers for their skilful contributions to the selection of the manuscripts for this special issue.