D01.6 Final Reports: "Final plan for using and disseminating the knowledge"

Project number	IST-027635
Project acronym	OpenTC
Project title	Open Trusted Computing
Deliverable Type	Report

Reference number	IST-027635/D01.6/FINAL V1.1
Title	D01.6 Final Reports: "Final plan for using and disseminating the knowledge"
WPs contributing	WP01
Due date	April 2009 (M42)
Actual submission date	June 03rd, 2009

Responsible Organisation	TEC
Authors	TEC plus contributions from all partners
Abstract	This document describes the main dissemination activities including exploitable knowledge of the OpenTC consortium during the project duration. It also outlines the planned activities beyond the project end.
Keywords	OpenTC, Dissemination, Trusted Computing, Exploitable Knowledge, Publications

Dissemination level	Public
Revision	Final V1.1

Instrument	IP	**Start date of the project**	1st November 2005
Thematic Priority	IST	**Duration**	42 months

If you need further information, please visit our website www.opentc.net or contact the coordinator:

Technikon Forschungs-und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel.+43 4242 23355 –0
Fax. +43 4242 23355 –77
Email coordination@opentc.net

Table of Contents

Index of Tables

Preface:

The purpose of dissemination is to **raise the awareness and publicity of the OpenTC project** as well as its results in order to make OpenTC a successful and sustainable project.

The target groups for external dissemination activities are on the one hand the general public and on the other hand potential business partners as well as specific scientific experts. A further target are public institutions like governmental and European audiences. In order to reach the particular awareness level intended, the **partners have to work continuously in the field of dissemination and public relation,** also beyond the project end. For their support as well as for the graphical identity within the consortium the partners have been provided with templates (for presentations and reporting) and various communication materials (web site, fact sheet, press release etc.).

The purpose of this plan is to collect information on the dissemination activities already done or concrete planned beyond the 42 month run time of the OpenTC project. It contains a plan for carried out and prospectively upcoming activities based on a form collected from each partner; it describes the used dissemination channels and materials and indicates their schedule.

1 Section 1 – Exploitable knowledge and its use

1.1 Introduction

Throughout the 42 months of the OpenTC project, partners have carried out numerous dissemination activities. Each partner is keeping track of its knowledge use and exploitation plans and activities which are regularly included in the wholesome project Dissemination plan. The deliverable describes the currently available results of the OpenTC project as well as the dissemination and exploitation actions that have taken place or are planned to take place in the near future.

1.2 Overview of exploitable knowledge

During the years of the OpenTC project, the project partners achieved a respectable amount of exploitable knowledge. The details of the products including their patents or other IPR issues are listed below.

Exploitable Knowledge	Exploitable products or measures	Sector(s) of application	Date of commer-cial use	Patents or other IPR protection	Owner/ partners involved
Basic and enhanced Trusted Computing enablement in product	Code, Concepts, Architectures, Use Case in prototype. Functionality integrated into product codebase	Enterprise customer	2009	None	IBM, HP, SUSE
Certificate service provider management application	MEITC CA component	Certificate management	2008	N/A	TUB
Command line and library utilities to interact with the system's TPM and a privacy CA, with imple-mentation of DAA – FINAL RELEASE	POL/OpenTC Trusted Platform Agent (TPA)	Software development	2009	None, open source	POL
DAA prototype implementation	IAIK DAA	Software development	2009	None, open source	IAIK
Expertise in trusted computing	Introduction of a new 'security-focused'	Higher education	09/2009	N/A	RHUL

Exploitable Knowledge	Exploitable products or measures	Sector(s) of application	Date of commer-cial use	Patents or other IPR protection	Owner/ partners involved
technology	undergraduate degree in computer science. As part of this undergraduate degree program a course in trusted computing will be offered in 2009/10, again building directly on the dissemination materials developed within the OpenTC project.				
Deep understanding of trusted computing and its applications	11-week MSc level course on Trusted Computing	Higher education	Yearly (since 2007)	None, open source	RHUL (support by HP and CUCL)
Deep understanding of trusted computing and its applications	11-week BSc final-year level course on Trusted Computing	Higher education	January 2010	None, open source	RHUL
DRM system and compartment integration	DRM core & DRM enabled video player	Digital media management	Not planned	MPEG-21	LDV, VLC deve-lopers
Encrypted File Service and related tools	Encrypted file service, key escrow tool, backup and recovery Tool	Defence, Medical, Financial	2010/11	GNU GPL	PORT
Enhancement of TLS- with DAA client authentication - FINAL RELEASE	POL/OpenTC Enhancement of OpenSSL (DAA engine)	Software development	2009	None, open source	POL
Expertise in trusted computing technology	Delivery of masters level course in TC	Higher education	01/2007	N/A	RHUL

Exploitable Knowledge	Exploitable products or measures	Sector(s) of application	Date of commer-cial use	Patents or other IPR protection	Owner/ partners involved
Framework for security management	Technology developed under OpenTC is expected to influence IBM's system management products	Data Centre management, Corporate computing at home	Post 2009	Protected	IBM (owner)
Graphical user interface of a TC-secured hypervisor	Hypervisor software	Virtualisation enhanced hardware	N/A	Patent protection being considered	ITAS
GUI for Trusted Virtual Client	Concept / Code	Business client platforms	2009/10	None	HP
Implementation of a TLS-based Trusted Channel FINAL RELEASE	POL/OpenTC Enhancement of OpenSSL (DAA engine)	Software development	2009	None, open source	POL, RUB
Implementation of JSR 321	IAIK jTSS-321	Software development	2009	None, open source	IAIK
Java Proxy with attestation support	IAIK proxy	Software development	2007	None, open source	IAIK
Libraries for Trusted Virtual Platform (TVP) components to allow TPM access	HIM TPM layer	Software development	2008	None, open source	TUD
Libraries to allow access to input devices in Xen MiniOS	Xen input drivers for SUI component	Software development	2008	None, open source	TUD, HP
Libraries and services to make secure standard application (protection of keys and configuration files) – FINAL RELEASE	POL/OpenTC Key Management Adaptation service (KMA)	Software development	2009	None, open source	POL
MPEG-A – Open Access Application	Publication and exchange system	Publication and academic sector	Not planned	Patents on MPEG standards	LDV

Exploitable Knowledge	Exploitable products or measures	Sector(s) of application	Date of commer-cial use	Patents or other IPR protection	Owner/ partners involved
Format					
MPEG-21 License parsing	DRM Core Compartment	Digital Rights Management	N/A	N/A	LDV
Native Java Implementation of the TCG Soft-ware Stack (TSS)	IAIK jTSS	Software development	2008	None, open source	IAIK
Network security management	Xen hypervisors	System management	Approx. 2008	None	IBM, HP
New super-conductive Nb-Ti alloy	MRI equipment	Medical, industrial inspection	2007, 2008	Patent planned for 2006	TUB
Object oriented Java API for interaction with the TCG Software Stack (TSS) for Java applications, UPDATE	IAIK/OpenTC Java TSS Wrapper	Software development	2008	None, open source	IAIK
On-the-fly video decryption for MPEG-4/21 files	DRM Player Compartment	Digital Rights Management	N/A	N/A	LDV
Password management system	Hypervisor software	Virtualisation enhanced hardware	N/A	Patent protection considered	ITAS
Java Privacy CA implementation running in XEN-compartment	PrivacyCA in a box	Software development	2009	None, open source	IAIK
IAIK/Java VM for TCP Implementations	TCPVM	Software development	2008	None, open source	IAIK
Patch to the OpenJDK providing basic services to extend the chain-of-trust to the managed Java environment	IAIK TCPVM	Software development	2008	None, open source	IAIK
PCA service running in a mini-malistic (Java)	PrivacyCA v2 in a Box	Software development	2009	Software development	IAIK

Exploitable Knowledge	Exploitable products or measures	Sector(s) of application	Date of commer-cial use	Patents or other IPR protection	Owner/ partners involved
compartment					
PrivacyCA implementation	IAIK privacyCA	Software development	2008	None, open source	IAIK
Static C code analyser	CAVEAT	Safety-critical sectors (aeronautics, space,railways, nuclear power plants, medical devices)	Currently undefined (point-wise agreements)	Deposit of a CAVEAT version at an usher	CEA
Secure Initialization Prototype (DRTM)	Secure intitalization of an AMD based PC platform using hardware support on the platform, integration with OS software	Computers, Security, Trusted Computing	2006 - ongoing	N/A	AMD
Secure initialisation prototype	Software proto-type and archi-tecture specifi-cation as basis for the standard	IT Security	2010	None	N/A
Security Methodology	Testing security, audits, frameworks	Any	2009	None, open source	ISE
Security metrics	Auditing Services, Procurement Services, Product Labelling	I.T., Banking, Consultancy, Finance/ Auditing	2008	None, open source	ISE
Set of command line utilities to interact with the system's TPM, UPDATE	IAIK/OpenTC Java TPM Tools (jTPM-Tools)	Software development	2008	None, open source	IAIK
Set of applications enhanced with KMA – FINAL RELEASE	OpenSSH, Ipsec setkey utility, Racoon (IKE), OpenSSL engine, PKCS#11 interface	Software development	2009	None, open source	POL
Source Code Metrics	Measuring security	N/A	2009	None, open source	ISE

Exploitable Knowledge	Exploitable products or measures	Sector(s) of application	Date of commer-cial use	Patents or other IPR protection	Owner/ partners involved
	complexity in source code				
Static C code analyser	FRAMA-C	Safety-critical sectors (aeronautics, space,railways, nuclear power plants, medical devices)	Undefined	Patent "PROCEDE ET SYSTEME DE VERIFICATION DE PROP-RIETES D'UN PROGRAMME INFORMATIQU E" BD1710 filed in France (no. 0700557)	CEA
Storage security management	Xen Hypervisor	System management	2008	None	IBM
TC-supported virtualization	Architecture, concept-bound image building. Embedded hypervisor in client- and server platforms supported by Linux in dom0.	Enterprise customer, interested consumer	2009	None	SUSE
Teaching of TC and its associated technologies, including the OpenTC demon-strator prototype	Tutorial documents (papers, book chapters, presentations), and HOW-TOs	Higher education, professional training	N/A	N/A	RHUL
Testing experience in automated TSS security testing	TCG Software Stack (TSS) Security and Robustness Test Suite	IT (Trusted Computing)	2008	None yet	BME (coop. with SEARCH-LAB Ltd.)
Testing experience in the automated security testing of XEN Hypervisor	XEN Hypervisor Security and Robustness Test Suite	IT (Trusted Computing)	2008	None yet	BME (coop. with SEARCH-LAB Ltd.)
Testing experience in the security testing of Trousers	Trousers Security and Robustness Test Suite	IT (Trusted Computing)	2008	None yet	BME (coop. with SEARCH-LAB Ltd.)

Exploitable Knowledge	Exploitable products or measures	Sector(s) of application	Date of commer-cial use	Patents or other IPR protection	Owner/ partners involved
Testing experience in the security testing of L4 microkernel	L4 Security and Robustness Test Suite	IT (Trusted Computing)	2009	None yet	BME (coop. with SEARCH-LAB Ltd.)
Tool to create special types of certificates and certificate exten-sions as specified by the Trusted Computing Group UPDATE	IAIK/OpenTC TCcert	Software development	2008	None, free for research, education and evaluation	IAIK
TPM secure firmware update, Linux	Secure firmware update program	TC developers, system integrators, IT departments	Since 2008	License contract	IFX
TPM test software Tool4TPM, Linux	Low level test program for platform verification	TC developers, system integrators, developers	Since 2008	License contract	IFX
TPM Software stack (TSS) Linux	TSS as licensable code	TC system integrators	Since 2008	License contract	IFX
Trust Metrics	Computerized Trust decision making	Sales, Auctions, Financing, Loans	2010	None, open source	ISE
Trusted Computing trust domain concepts (TvD)	Code, Concepts, Architectures, Applied Use Case in prototype. Vswitch, trusted GUI	Enterprise customer	2009	None	SUSE
Trusted email framework	MEITC	Software development	2009	None	TUB
Trusted mail management software	MEITC web management	Software development	2009	None	TUB
LibVirt Security Architecture	Management standardization	IT	2009	None	IBM
User interface for TC-supported	N/A	IT	N/A	N/A	ITAS; to be used

Exploitable Knowledge	Exploitable products or measures	Sector(s) of application	Date of commercial use	Patents or other IPR protection	Owner/ partners involved
virtualisation					by all partners
XIDC management extension for generic XEN IPC based, network like communication in XEN	Prototype library	Universal (OS Virt)	2008	None, intended release as OSS	HP
Security service: virtual switch for XEN inter-domain communication	Prototype implementation	Universal (OS virt)	2008	None, intended release as OSS	HP, RUB
Security service: GUI for XEN (client platforms, management consoles)	Prototype implementation	Universal (OS virt)	2009	None, intended release as OSS	HP, RUB, CUCL
Management infrastructure for trusted virtualized clients	Platform components for management	Managed corp. PCs	2011	n.a. (software)	HP
Trusted virtualized client architecture	PCs and Notebooks with embedded hypervisors	Universal	2011	trade-marked	HP
Virtual TPM for L4.Fiasco/L4Env platform	VTPM for L4.Fiasco/L4Env and future platforms	Software development	2008	None, open source	TUD
XKMS PKI protocol implementation, release and UPDATE	IAIK XKMS	Software development	2008	None, free for research, education and evaluation	IAIK

Table 1: Exploitable knowledge achieved

1.3 Description of results

The main outcomes in exploitable knowledge are described below:

1.3.1 OpenTC Java TPM Tools (jTPM-Tools)

The jTPM Tools provide a set of command line utilities to interact with the system's TPM. The tools are based on the IAIK/OpenTC jTSS Wrapper and the IAIK/OpenTC TCcert library (developed in WP05). The most important features, distinguishing the jTPM Tools from other TPM utilities, are the ability to create Attestation Identity Keys (AIKs) and AIK certificates as well as the ability to extract the Endorsement Key (EK) certificates from Infineon 1.1b and 1.2 TPMs. In year two several new versions of the jTPM-tools have been published, adding PKI-functionality and integrating support for new versions of software stacks used.

1.3.2 OpenTC Java TSS Wrapper

Trusted Computing, as specified by the Trusted Computing Group (TCG) (http://www.trustedcomputinggroup.org/), comprises multiple layers of hard- and software. While the hardware consists of the Trusted Platform Module (TPM) and related trusted building blocks, the main software components include the TPM hardware driver and a Trusted Software Stack (TSS). This TSS is typically developed in pure C and can therefore not directly be used from other languages such as Java. For that reason, the IAIK/OpenTC jTSS Wrapper provides language bindings for Java via the Java Native Interface (JNI). The goal is to make the Trusted Service Provider Interface (TSPI) of the TSS stack available to Java developers in an object oriented fashion. Much of the required functionality was already developed during year one. Later on, most of the changes were bug fixes, API-adaptations and workarounds necessary to access the Infineon-stack. This is necessary since the TSS-specification is written with sufficient flexibility allowing implementers to come up with different variations still claiming to be con formant to the standard. Currently different updates on the jTSS Wrapper were made. One important update is to allow jTss Wrapper to be build with current TrouSerS 0.3.1cvs.

1.3.3 OpenTC Tccert

IAIK/OpenTC TCcert is a software tool which enables one to create special types of certificates, as specified by the Trusted Computing Group. TCcert implements the "TCG Infrastructure Credential Profiles" document and supports the TPM Endorsement Key (EK), Platform Endorsement (PE) and Attestation Identity Key (AIK) credentials. TCcert also allows to build the Subject Key Attestation Evidence (SKAE) extension for certificates, both in plain and encrypted format.

1.3.4 XKMS

IAIK has developed an implementation of the XML Key Management Specification (XKMS) (http://www.w3.org/TR/xkms2/). As suggested by the TCG in their "Reference Architecture for Interoperability" document: "XKMS provides the most attractive solution for credential management for existing CAs in the PKI industry." Thus, XKMS is a prime candidate as a foundation of a Trusted Computing enabled public key infrastructure. This release so far does not contain the Trusted Computing specific classes. It is a generic build, intended to stimulate public interoperability testing with other XKMS implementations. Several bugfix updates were also made.

IAIK XKMS is available for download at the Trusted Java Sourceforge website at:

http://trustedjava.sourceforge.net

1.3.5 jTSS

To provide pure Java access to TPMs for applications, we have developed on a pure Java version of jTSS.

The IAIK jTSS stack is an implementation of the TCG Software Stack for the Java™ programming language. In contrast to approaches like the IAIK/OpenTC jTSS Wrapper, the IAIK jTSS does not wrap a C stack like TrouSerS but implements all the TSS layers in Java™. For this stack we followed the TSS-specifications of the TCG but will also investigate other ways to provide TSS functions to applications. The first version has been published by the end of April 2007 and an update has been made available in September 2007. Implementation of SOAP-support has also been finished. Until December 2008 several new features have been incorporate in jTSS 0.4. The changes include support for NV access, key migration, CMK, a new event log, an alternative SQL-Database for Persistent Storage, support for monotonic counters, more tests, a TrouSerS key import tool and a new Windows installer that eases deployment of trustedJava applications. The updated version of the JTSS is now available for download.

This implementation supports the Infineon 1.2 TPM and is also compatible with most of the following common TPMs: Infineon 1.1b, Broadcom 1.2, ST Microelectronics 1.2, Atmel 1.1 and the software TPM emulator. The stack also demonstrates the platform independence of Java as it is usable under Linux as well as Windows Vista.

1.3.6 PRIVACYCA

The Trusted Computing team of IAIK releases a basic PrivacyCA 0.1 implementation, utilizing EK and AIK certificates, plus minimal PKI operations (e.g. Issue, locate, validate, revoke). Note that the emphasis is on basic. This is a proof-of-concept implementation of the mechanics, to gain experience of the issues involved. A future advanced TC PKI design is expected to improve on the current design.

Now another Trusted Computing PKI (APKI) package to run a PrivacyCA is released.

This is a redesigned version of the functionality provided in the 0.1 release. It was optimised to be as small as possible, thus doing away with the XKMS and XML overheard and using a much simpler protocol. This release allows to run the PrivacyCA Java server in a 17Mb Xen compartment (build instructions included). Further, commandline demonstration clients for jTSS (Java) and TrouSerS (C) are provided.

All required software packages are available from http://trustedjava.sourceforge.net/.

For your testing curiosity, a basic set-up is running at http://opentc.iaik.tugraz.at/.

1.3.7 Java Tools Update

IFX 1.2 TPM patch for TrouSerS 0.2.9: Just days after TrouSers 0.2.9 was released the IFX 1.2 DUAL patch is ready.
jTSS Wrapper 0.2.5 + jTpm Tools 0.2: Also, the Java Wrapper plus demonstration tools were updated and should work just as fine as they did with TrouSerS 0.2.8.
IAIK XKMS 0.2: On the PKI side the XKMS protocol implementation received a major overhaul.
Documentation and source code are available at the Sourceforge website at:
http://trustedjava.sourceforge.net

IAIK XKMS 0.1 is developed and maintained at the Institute for Applied Information Processing and Communication (IAIK) (http://www.iaik.at) at Graz University of Technology.

1.3.8 New set of Java Software Packages

IAIK Trusted Computing labs release a new set of software packages to support Trusted Computing with the Java(tm) programming language.

JTSS 0.1: The IAIK jTSS stack is an implementation of the TCG Software Stack for the Java(tm) programming language. In contrast to the approach of the jTSS Wrapper, jTSS does not wrap a C stack like TrouSerS but implements all the TSS layers in 100% Java(tm). This is the first public release of IAIK jTSS and it is still in early stages of development. It is currently regarded as experimental software targeted at research and educational environments.

jTss Wrapper 0.3: Beginning with version 0.3, IAIK/OpenTC jTSS Wrapper is no longer a standalone package, but is an add-on to the IAIK jTSS.

IAIK/OpenTC jTSS Wrapper provides Java(tm) bindings for the TrouSerS TSS. To make switching between the wrapper and the full jTSS stack as simple as possible, both packages employ the same API.

JTpmTools 0.3: The IAIK/OpenTC jTpmTools are a set of command line tools demonstrating basic interaction with the Trusted Platform Module (TPM) and the Trusted Software Stack (TSS). This includes tools for taking/clearing ownership and reading/extending PCRs. Also, commands for managing keys and binding/sealing of data blocks are available. Further, commands for creating Attestation Identity Keys (AIKs) and interaction with a remote PrivacyCA service (to obtain accompanying certificates) using the XKMS protocol are included.

TCcert 0.2.2: This release synchronizes TCcert with the new releases of jTpmTools and jTss.
Documentation and source code are available at the Sourceforge website at:
http://trustedjava.sourceforge.net

1.3.9 Graphical user interface of a TC-secured hypervisor

Problem: As hypervisors and PCs with TPMs will increasingly be used, both normal users and administrators will have a need to handle these conveniently and securely. Based on findings from an expert survey, ITAS developed characteristics of the user interface of a hypervisor such as the OpenTC prototype. The requirements are that the user interface should be easy to handle (similar to today's user interfaces), graphical (for ease of use), the graphics should be on the usual screen (as special screens etc. would be overlooked), the user interface should help the user in managing his security and the security of business partners and employers.

Solution: A GUI which has similarities with existing GUIs of operating systems, but also differences, in particular concerning the security aspects, so that users can tell between the new interface parts and ones from the legacy OS. Switching between operating systems should therefore be similar to switching between applications, but in new type of separate task bar. Security is ascertained by a sealed image in the same separate task bar, which is only shown if the hypervisor is in a proper state. Control of the hypervisor (and the TCB) is similar to the control of a normal operating system, with e.g. providing a desktop or context menu, in new forms, though. The innovative desktop of the hypervisor provides easy control over the installed or running operating systems, system resources, security status, etc. Some compartments could even be secured or displayed as securely isolated by the hypervisor/TCB, even if their contents not in certified. In this case, users can e.g. define that they are displayed with a green light, or users could define that they are secure for their purposed when booted (for subsequent deletion). Traffic-light symbols or other visualisation could be used.

The innovative user interface could be used throughout the IT industry, from server systems to mobile phones.

1.3.10 Password Management System

Problem: Users may increasingly use different instances of operating systems on the same machine. This increases the problem for the user of securely handling all these passwords. The problem is aggravated by the need to securely handle other passwords, e.g. to VPN-access.

Solution: A password management system has to authenticate the user and help the user in managing IDs and passwords. The system should allow to manage the service, e.g. to configure it (e.g. which password links to which operation) and to delete, change, view history, export, backup, restore data, etc. Passwords for other operations (e.g. mobile phone) could be managed by the same service. Some processes might be given access to part of the service if they can authenticate

themselves. The password management system should be able to handle different users on the same machine and store their information in separate encrypted files. The password management system may need to run in its own encrypted compartment.

The system could be used with any computer, but in particular with any hypervisor-based system. The system itself doesn't need on-line access. If on-line access is available, the integrated backup-system could send the encrypted backup-files automatically to a backup-server.

2 Section 2 – Dissemination of knowledge

2.1 Introduction

In the beginning of the project the OpenTC partners developed a dissemination and use plan which describes both the strategies and activities of the consortium in general as well as the individual dissemination approaches of the partner organisations. This document takes a look at the dissemination activities already carried out, but also at the activities planned in the future, beyond the project end. The consortium strived to promote and encourage research about OpenTC, targeting European companies and citizens by the diffusion of information about the project as well as state-of-the-art and evolution of related technologies.

The overview below contains a summary of all dissemination activities that were carried out and reported during the whole project.

Later in the document the activities are detailed in a more comprehensive manner and the major activities are detailed further.

In brief, the amount of different dissemination activities summarised in the following table:

Activity Type	International	National
Conferences	64	1
Workshops	20	10
Presentations	27	10
Discussions	22	4
Courses	22	9
Other	7	1

Table 2: Amount of different dissemination activities

It can be seen from this table that the majority of the dissemination activities have taken place in international contexts. As the activity types are self-explanatory, they will not be described here in further detail. In addition to their international nature, consortium partners have carried out the dissemination activities in cooperation. The OpenTC project has been communicated in paper and electronic media in different ways as well as in various conferences, summits, workshops and seminars by active participation in the organisation of these events or through invited speakers or conference paper contributors.

2.2 Overview of conferences, public discussions and talks

The dissemination activities of the OpenTC consortium are collected below and listed in a chronological order.

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
20/02-21/02/2006	Workshop "Fostering a European Academic Research Environment for Trusted Computing" organized by the British CESG and German BSI	Higher education, research	Europe	9	RHUL, RUB, TUD, HP, CUCL
23/02/2006	Lecture on Trusted Computing for MSc in Information Security – Software security course	Higher education	Europe	40	RHUL
24/02-01/03/2006	Analysis and discussion of TC, and presentation of OpenTC views (indicare Monitor)	Industry	Inter-national	N/A	LDV, HP, ITAS, TUM
14/03/2006	Presentation on Trusted Computing Platforms at STMicroelectronics Belgium	Industry	National, Belgium	35	KUL
20/03/2006	BrainShare, Salt Lake City	Industry, Professionals	Inter-national	45	SUSE
31/03/2006	EUROSEC2008 European Workshop on Systems Security	Higher education	Inter-national	20	BME
26/04/2006	TRECK (Trust, Recommendations, Evidence and other Collaboration Know-how) track at: 21st ACM Symposium on Applied Computing	Higher education, research	Inter-national	30	RHUL
06/05/2006	Talk: "Overview of Xen 3.0 and architecture" LinuxTag	Industry, community	National, Germany	100	HP, TEC, CUCL, SUSE
16/05-19/05/2006	Fourth iTrust International Conference on Trust Management	Research, industry	Inter-national	N/A	RHUL
19/05/2006	Grazer Linux Tag 06	Public, industry	National, Austria	30	IAIK
22/05/2006	I-NetSec 2006 in conjunction with IFIP TC 11's SEC'2006	Industry	Inter-national	100	BME
02/06/2006	Wiener Linuxwochen 06	Industry, community	National, Austria	80	IAIK

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
17/07-28/07/2006	IPICS Summer Course	Academia, Industry	National, Belgium	144	KUL, IAIK, RHUL
20/07-21/07/2006	Participation in discussion and research presentation: CERICS: "Workshop on Current and Emerging Research Issues in Computer Security"	Higher education, research	Europe	50	RHUL
31/07-04/08/2006	Usenix Security	Higher education	Inter-national	N/A	CUCL
19/08-25/08/2006	1st European Trusted Infrastructure Summer School (ETISS) – Oxford, UK	Higher education	Inter-national	N/A	RHUL, RUB, HP, CUCL, TUD, POL
23/08/2006	Tutorial presentation on Trusted Computing at the Information Security Summer School, Taipei, Taiwan	Higher education, research	Inter-national	60	RHUL
07/09–08/09/2006	Xen Summit, San Jose, CA	Industry	Inter-national	150	CUCL
11/09/2006	OSS Developer conference, Harrachov, CZ	Linux and OSS developers	Europe	31	SUSE, HP
13/10/2006	Presentation to the „Gesellschaft Informatik" at Fuji-Siemens in Munich	Higher education, Industry	Europe	40	CUCL
16/10/2006	Network Security Innovation Platform Workshop (UK Government Department of Trade and Industry)	Research, industry	National, UK	50	RHUL
19/10/2006	11th Nordic Workshop on Secure IT Systems	Higher education	Inter-national	50	BME
21/10/2006	CMS eUniversity Workshop	Academic	Inter-national, Greece	15	IAIK
30/10-03/11/2006	Conference/Workshop "ACM CCS / STC 2006"	Research	Inter-national	40	RUB
11/2006	A.-R. Sadeghi, M. Scheibel, S. Schulz, C. Stüble, M. Wolf, 'Play it once again, Sam -	Higher education, Industry	Inter-national	40	RUB

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
	Enforcing Stateful Licenses on Open Platforms' - Accepted forpresentation at The Second Workshop on Advances in Trusted Computing (WATC '06)				
11/2006	H. Löhr, H.G.V. Ramasamy, S. Schulz, M. Schunter, C. Stüble, 'Enhancing Grid Security Using Trusted Virtualisation', Accepted to be presented at The Second Workshop on Advances in Trusted Computing (WATC '06 Fall)	Higher education, Industry	Inter-national	40	RUB
11/2006	L. Chen, R. Landfermann, H. Löhr, M. Rohe, A.-R. Sadeghi and C. Stüble, 'A Protocol for Property-Based Attestation', Accepted for The First ACM Workshop on Scalable Trusted Computing (STC'06)	Higher education, Industry	Inter-national	N/A	RUB
11/2006	A.-R. Sadeghi, M. Selhorst, C. Stüble, C. Wachsmann and M. Winandy, 'TCG Inside?- A Note on TPM Specification Com-pliance', Accepted for The First ACM Workshop on Scalable Trusted Computing (STC'06)	Higher education, Industry	Inter-national	N/A	RUB
11/2006	Participation IST Event Helsinki	Industry, government, higher education, research	Europe	N/A	TEC
06/11-08/11/2006	OSDI in Seattle, USA	Research	Inter-national	N/A	TUD
07/11/2006	Open Source Business Forum in Potsdam	Industry	Inter-national	120	CUCL
14/11/2006	Linux World Expo, Cologne	Industry	Inter-national	N/A	CUCL
08/11-09/11/2006	IT Security National Summit, Ireland	Industry, professionals, government	Europe	N/A	RUB
14/11-17/11/2006	Software Defined Radio Technical Conference 2006 – Invited paper : "Trusted Com-	Research, Industry	Inter-national	200	RHUL

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
	puting Technologies and their use in the Provision of High Assurance SDR Platforms"				
30/11-01/12/2006	Workshop "WATC"	Research	Inter-national	40	RUB
01/12/2006	Workshop on vulnerabilities and defence techniques	Industry, professionals	Italy	~50	POL
18/12/2006	HP Day at RHUL; OTC booth at HP colloquium	Industry, higher education	Europe	100	RHUL, HP
01/2007	HPLabs research show and tell	Analysts	Europe	15	HP
2006-2007	RHUL Trusted Computing discussion group: 4 1-hour tutorials and weekly 1-hour discussion sessions.	Research	Europe	7	RHUL
11/01-12/01/2007	IEEE CCNC Conference 07; Efficient design of interpretation of REL license using Expert Systems	Research, industry	Inter-national	30	LDV
18/01/2007	EC Expert workshop on Trusted Computing	Research, government	Europe	20	HP
31/01/2007	Solutions Linux, Paris	Professional Linux/Unix users	National, France	22	SUSE
02/2007	Lectures at RHUL	Higher education	National, UK	50	CUCL
07/02/2007	Workshop on security for business applications	Industry, professionals	National, Italy	~100	POL
15/02/2007	Lecture on Trusted Computing for MSc in Information Security – Software Security Course	Higher education	Inter-national	40	RHUL
20/02/2007	Presentation of OpenTC to POL's research groups involved in RE-TRUST project	Higher education	Inter-national	10	POL
26/02-27/02/2007	EU Workshop "Deployment of TC for Government Organisations"	Research, government	Europe	100	RUB
26/02-27/02/2007	Workshop on Trusted Computing from a European Perspective – Trusted Computing activities in Italy –	Research, industry, government	Europe	80	POLITO, HP, RUB, IFX,

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
	Bonn, Germany				TEC, TUD
03/2007	Research Talk	Higher education	National, UK	50	CUCL
06/03/2007	ISECOM Subscriber discussions	Professionals	Inter-national	1000	ISE
15/03-21/03/2007	Presentation of Significant European Projects on TC at CeBIT (OpenTC, EMSCB)	Industry	Inter-national	55	RUB
20/03/2007	RE-Trust workshop. RETRUST project; this is an EU-funded research project lead by the University of Trento on Remote EnTrusting by Run-time Software auThentication. http://retrust.dit.unitn.it/	Higher education, industry	Europe	N/A	HP
21/03/2007	BrainShare, Salt Lake City	Industry Professionals	Inter-national	33	SUSE
21/03/2007	Seminar given at the Department of Computer Science and Software Engineering, University of Canterbury, New Zealand, entitled: "Trusted Computing: A universal security infrastructure?"	Higher education, research	Inter-national; New Zealand	25	RHUL
21/03-23/03/2007	EuroSys 2007	Research	Inter-national	N/A	TUD
23/03-25/03/2007	European Conference on Security Research, http://www.src07.de/ Invited panellists	Industry, higher education, government	Inter-national	1000	HP
28/03/2007	C. J. Mitchell: Talk to the New Zealand Information Security Forum, Auckland, New Zealand, entitled: "Trusted Computing: Putting a Security Module on Every Desktop".	Industry	Inter-national; New Zealand	25	RHUL
28/03/2007	C. J. Mitchell: Seminar given at the Centre of Digital Enterprise (CODE), University of Auckland, New Zealand, entitled:	Higher education, research	Inter-national; New Zealand	20	RHUL

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
	"Trusted Computing: A Universal Security Infrastructure?".				
23/04-26/04/2007	HP TechCon 2007. Internal HP technology conference. Presented poster session on Trusted Infrastructure that included OpenTC	Research	Inter-national	200	HP
05/2007	Grazer Linux Tag 07	Industry, community	National, Austria	N/A	IAIK
03/05/2007	TPM and TC Presentation at the Teletrust Workshop	Research, industry, Teletrust members	National, Germany	25	IFX
05/05-06/05/2007	FP7 Security Workshop (national conference on security projects)	Higher education	National, Turkey	70	TUB
08/05-10/05/2007	International Conference on Security of Information and Networks (Sinconf 2007)	Higher education, industry	National, Turkey	100	TUB
21/05-23/05/2007	Presentation at UbiSafe Computing 2007 - The 2007 IEEE International Symposium on Ubisafe Computing, Ontario, Canada, entitled "Mobile Agents and the Deus Ex Machina".	Higher education, research	Inter-national	20	RHUL
21/05–24/05/2007	E. Cesena, P. C. Pomi, G. Ramunno, D.Vernizzi "Performances of Xen's Secured Virtual Networks." - TERENA Networking Conference 2007 (TNC2007)	N/A	Europe	N/A	POL
24/05/2007	Presentation at Cast Forum, Darmstadt, Germany	IT-professionals	National, Germany	50	ITAS
06/2007	Feedback on www.opentc.net	Public	Inter-national	N/A	TEC
10/06/2007	Presentation of Open Trusted Computing project during monthly TUBITAK seminars on security	TUBITAK staff	Turkey	40	TUB
22/06/2007	PET2007	Research	Inter-national	100	IBM

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
07/2007	S. Lo Presti; 'A Tree of Trust rooted in Extended Trusted Computing' in Proc. Of ACSF (Advances in Computer Security and Forensics) 2007 Conference	Research	Inter-national, UK	50	RHUL
07/2007	H. Löhr, H.G.V. Ramasamy, A.-R. Sadeghi, S. Schulz, M. Schunter, C. Stüble, 'Enhancing Grid Security Using Trusted Virtualisation', Accepted for The 4th Inter-national Conference on Autonomic and Trusted Computing (ATC-07)	Higher education, Industry	Inter-national	N/A	RUB
04/07-06/07/2007	ECRTS 2007	Research	Inter-national	N/A	TUD
10/07-13/07/2007	International Course on State of the Art and Evolution of Computer Security and Industrial Cryptography 2007	Research, industry, government	National, Belgium	50	KUL
11/07-13/07/2007	Conference "ATC 2007"	Research	Inter-national	40	RUB, IBM
27/07/2007	S. Lo Presti, ''A Tree of Trust rooted in Extended Trusted Computing', National Research Council of Canada (NRC), Information Security Group	Research	Inter-national, Canada	8	RHUL
29/07-03/08/2007	Workshops and tutorials at the IFIP Trust Management 2007 Conference	Industry, government, higher education, research	Inter-national, Canada	100	RHUL
30/07-02/08/2007	IFIPTM 2007 - Joint iTrust and PST Conferences on Privacy, Trust Management and Security, Moncton, New Brunswick, Canada.	Higher education, research, Industry	Inter-national	N/A	RHUL
07/08/2007	C. J. Mitchell, 'Trusted mobile platforms', Two half-day ses-sions given at: ISSS '07, In-formation Security Summer School	Higher education, research	Inter-national, Taiwan	55	RHUL
08/08-	Usenix Security 2007	Research,	Inter-	N/A	TUD

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
10/08/2007		industry	national		
18/08/2007	Innovation Days	Defense	National, Germany	50	IBM
25/08/2007	News List	Professionals	Inter-national	30000	ISE
03/09/2007	Presentation to Australian Government	Government	Australia	10	HP
05/09-06/09/2007	E. Gallery and C. J. Mitchell, 'Trusted mobile platforms', Two half-day sessions given at Foundations of Security Ana-lysis and Design: FOSAD 2007	Higher education, research	Italy	50	RHUL
09/09-15/09/2007	Presentation at FOSAD 07 – The 7th International School on Foundations of Security Analysis and Design,Bertinoro, Italy, entitled: "Trusted Mobile Platforms".	Research	Inter-national	50	RHUL
12/09/2007	Innovation Event	Defense	Inter-national, Sweden	80	IBM
18/09/2007	Innovation Days	Defense	Inter-national, Germany	50	IBM
29/09-05/10/2007	2nd European Trusted Infrastructure Summer School (ETISS) – Bochum, Germany	Research, industry, government, higher education	Europe	100	IAIK, RHUL, RUB, POL, HP, TUD, KUL
10/2007	Discussions with HP OSC	Industry	Europe	N/A	HP
01/10-04/10/2007	EMSOFT	Research	Inter-national	N/A	TUD
08/10/2007 - 02/02/2008	University lecture"Microkernel-Based Operating Systems" - Lecture on design principles for secure systems and trusted computing applications	Higher education	Inter-national	20	TUD
10/10/2007	ISECOM Subscriber discussions	Professionals	Inter-national	1000	ISE
14/10-19/10/2007	Dagstuhl Seminar "Formal Protocol Verification Applied"	Research	Inter-national	35	RUB

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
15/10-17/10/2007	SOSP 2007	Research	Inter-national	N/A	TUD, CUCL
16/10/2007	Talk am DESIGN & ELEKTRONIK - Entwickler-forum: Trusted Hardware	Potential users and developers	Europe	30	IFX
25/10/2007	Presentation to Microsoft Research	Industry	Europe	2	HP
25/10-27/10/2007	MSIT2007 Security Conference,University Moscow, Russia - Invited Talk: «Доверенные вычисления: стандарты безопасности на базе платформ целостности и доверия» http://www.iisi.msu.ru/	Industry, higher education, government	Inter-national	200	IFX
29/10-05/11/2007	Conference/Workshop "ACM CCS / STC 2007"	Research	Inter-national	25	RUB
30/10/2007	CCS2007	Research	Inter-national	300	IBM, HP
11/2007	Trustworthy Global Computing (TGC 07)	Research	Europe	N/A	IAIK
11/2007	The Second ACM Workshop on Scalable Trusted Computing (STC'07)	Research; professionals	Inter-national	N/A	IAIK
11/2007	Summit Talk	Industry, higher education	Inter-national	150	CUCL
02/11/2007	T. Eisenbarth, T. Güneysu, C. Paar, A.-R. Sadeghi, D. Schellekens, M. Wolf: "Reconfigurable Trusted Computing in Hardware" - Accepted for ACM STC	Higher education, Industry	Inter-national	N/A	RUB
15/11/2007	DailyDave security list	Professionals	Inter-national	3000	ISE
15/11/2007	Xen Summit, Santa Clara - Talk: "Improving Xen security through domain-zero disaggregation".	Industry	Inter-national	100	CUCL
28/11-30/11/2007	AXMEDIS Conference 2007. Panel for Issues in security for Digital Rights Management.	Scientific community, research	Inter-national	40	LDV

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
09/12/2007	Innovation Event	Defense	National, Sweden	80	IBM
17/12/2007	OTC booth at HP colloquium at RHUL	Industry, Higher education	Europe	80	RHUL
12/2007	Two half-day sessions were presented at the University of Macquarie, Sydney, entitled: "Enabling Secure Download using Trusted Computing" & "Trusted Mobile Platforms".	Research	Inter-national	20	RHUL
2007	Internal presentation	Laboratories, department and company	CEA employees	N/A	CEA
2007	11 week MSc course in Trusted Computing	Higher education	Inter-national	20	RHUL
2007	Y. Gasmi, A.-R. Sadeghi, P. Stewin, M. Unger, N. Asokan, 'Beyond Secure Channels', Accepted for ACM STC (Scalable Trusted Computing)	Higher education, Industry	Inter-national	N/A	RUB
2007	N. Asokan, J.-E. Ekberg, A.-R. Sadeghi, C. Stüble, M. Wolf, 'Enabling Fairer Digital Rights Management with Trusted Computing', to be presented at ISC07, Information Security Conference 2007	Higher education, Industry	Inter-national	N/A	RUB
2007	S. Gajek, A.-R. Sadeghi, J. Schwenk and M. Winandy, 'Trusted User-Aware Web Authentication', Accepted for 3rd Workshop on Trustworthy User Interfaces for Passwords and Personal Information (TIPPI'07), Stanford (USA)	Higher education, Industry	Inter-national	N/A	RUB
2007	D. Birk, S. Gajek, F. Gröbert, and A.-R. Sadeghi, 'Phishing Phishers - Observing and Tracing Organised Cybercrime', Accepted for IEEE Workshop on Cyber-Fraud (Cyberfraud'07), Silicon Valley (USA)	Higher education, Industry	Inter-national	N/A	RUB

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
2007	S. Gajek, M. Manulis, A.-R. Sadeghi and J. Schwenk', Browser Models for Usable Authentication Protocols', Accepted for IEEE Security and Privacy, Web 2.0 Security and Privacy Workshop (W2SP'07), Oakland (USA)	Higher education, Industry	Inter-national	N/A	RUB
2007	D. Birk, S. Gajek, F. Grobert, and A.-R. Sadeghi, 'Phishing phishers - oberserving and tracing organised cybercrime', In IEEE Cyberfraud, 2007	Higher education, Industry	Inter-national	N/A	RUB
2007	S. Katzenbeisser, A.-R. Sadeghi, B. Skoric, M.Celik, 'Combining Tardos fingerprinting codes and fingercasting', Accepted for Information Hiding Conference (IH'07)	Higher education, Industry	Inter-national	N/A	RUB
2007	A.Adelsbach, U. Huber and A.-R. Sadeghi, 'Fingercasting - Joint Fingerprinting and Decryption of Broadcast Messages', Accepted for LNCS Transactions on Data Hiding and Media Security 2007	Higher education, Industry	Inter-national	N/A	RUB
2007	S. Gajek, A.-R. Sadeghi, C. Stüble and M. Winandy, 'Compartmented Security for Browsers - Or How to Thwart a Phisher with Trusted Computing', Accepted for The Second International Conference on Availability, Reliability and Security ARES 2007	Higher education, Industry	Inter-national	N/A	RUB
01/2008	Research seminar at Trinity Hall	Higher education	National, UK	30	CUCL
18/01/2008	1st COMMUNIA International Workshop (Technology and the Public Domain) http://ws1-2008.communia-project.eu/	Higher education, research, government	Europe	~100	POL
19/01-	SOFSEM 2008 conference	Research	Inter-	N/A	RUB

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
25/01/2008			national		
07/02/2008	Lecture on Trusted Computing for MSc in Information Security – Software security course	Higher education	Inter-national	40	RHUL
23/02/2008	FOSDEM 2008 Conference , Brussels - Seminar on Trusted Computing	Developers	Europe	120	TUB
26/02-28/02/2008	Trusted Computing Group face to face meeting, Tokyo: Trusted computing standardization	TC specialists researchers, developers	Inter-national	~150	IFX
03/03/2008	Invited talk at the Department of Computer Science, University of British Columbia, Vancouver: "Improving Xen security through disaggregation"	Higher education	Canada	10	CUCL
07/03/2008	ACM VEE 2008, Seattle - Talk: "Improving Xen security through disaggregation"	Higher education	Inter-national	50	CUCL
10/03-13/03/2008	Contributions to Trust 2008, Villach, Austria (tutorials, talks and presentations, papers, booths, organisation, ...)	TC- experts, higher education, industry,	Inter-national	~150	All partners
10/03-14/03/2008	An invited talk was presented at the TRUST2008 educational event titled "Who is the TCG and what are the TCG concepts?"	Higher education	Europe	40	RHUL
10/03-14/03/2008	An paper was presented at TRUST2008 entitled "On a possible privacy flaw in Direct Anonymous Attestation(DAA)"	Research	Europe	30	RHUL
12/03/2008	Talk within the TRUST conference	Technical experts	Inter-national	100	IAIK
13/03/2008	Course for professors of applied technological uni-versities: Trusted computing for embedded microelectronics with Megawirkung– Innovative Solutions for Energy Efficiency, Communication and Security	Higher education	National	~50	IFX

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
17/03/2008	BrainShare, Salt Lake City	Industry Professionals	Inter-national	38	SUSE
31/03/2008	EuroSec 2008, Glasgow - Talk: "Privilege separation made easy"	Higher education	Inter-national	15	CUCL
07/04-11/04/2008	RSA conference 2008 San Francisco, USA; Security and cryptography, Trusted Computing	TC experts, professionals	Inter-national	~8000	IFX
07/04 - 19/07/2008	University lecture "Distributed Operating Systems", introducing trusted computing paradigms to students	Higher education	Inter-national	20	TUD
18/04/2008	Output'08 - Open day at TUD's department of computer science http://output.inf.tu-dresden.de/	Students	Germany	10	TUD
20/04-26/04/2008	ISPEC 2008 conference	Research	Inter-national	N/A	RUB
05/2008	Professional course (Introduction to Trusted Computing)	Industry	National, Italy	~20	POL
07/05/2008	Technical Discussion	Java Experts	Inter-national	10	IAIK
08/05/2008	Workshop on electronic billing	Business and technical managers	National, Italy	~200	POL
12/05-13/05/2008	Research meeting jointly organised by Microsoft Research and HP Labs: "The Rise and Rise of the Declarative Datacenter"	Higher education	Inter-national	N/A	IBM, HP
19/5/2008	CCGrid 2008 Conference - Tutorial on "Trusted virtualization and grid security"	Developers	National; France	15	TUB, PORT
19/05-22/05/2008	Paper presented at WSES2008 - the 3rd International Work-shop on Workflow Systems in e-Science, Lyon, France, "Securing Grid Workflows with Trusted Computing"	Research	Europe	30	RHUL
28/05/2008	Presentation	Linux Experts	National,	100	IAIK

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
			Germany		
06/2008	Workshop / Presentation	Technical Experts	Inter-national	20	IAIK
23/06-25/06/2008	Paper presented at ICCS 2008 - the 8th International Conference on Computational Science: Applications of Work-flows in Computational Science Krakow, Poland, "Securing Grid Workflows with Trusted Computing"	Research	Europe	30	RHUL
30/06–02/07/2008	Contributions to the Future of Trusted Computing Conference, Berlin, Germany	Higher education, industry, public	Inter-national	~300	RUB, HP, IFX, IAIK
07/2008	Presentation	TC experts	Inter-national	100	ITAS
08/2008	Demonstration of OpenTC EFS to Turkish Defense Industry	Defense industry	National, Turkey	50	PORT
11/08-15/08/2008	Asia-Pacific TC Summer School Malaysia (keynote, presentation)	Higher education/ industry	Inter-national SE Asia	150	HP
20/08-24/08/2008	First Asia Pacific Trusted Infrastructure Summer School	Higher education, industry	Asian-Pacific Region	200	HP, RUB
23/08/2008	Public event at Linux Birthday Celebration by Chamber of Electrical Engineers	Linux and OSS community	National, Turkey	150	PORT
31/08-05/09/2008	3rd European Trusted Infrastructure Summer School (ETISS) – Oxford, UK	Higher education, industry, TCG member organizations	Europe	~100	POL, RUB,
08/09/2008	OSS developer conference Liberec, CZ	Linux and OSS developers	Inter-national	28	SUSE, IBM
08/09-10/09/2008	Paper presented at IAS 2008 - the 4th International Conference on Information Assurance and Security, Naples, Italy, entitled: "A Device Management Framework for Secure Ubiquitous Services Delivery"	Research	Europe	30	RHUL

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
15/09-18/09/2008	ISC 2008 conference	researchers	Inter-national	N/A	RUB
31/09–04/10/2008	An invited talk was presented at the 3rd European Trusted Infrastructure Summer School 2008 (ETISS 2008), Oxford, U.K., titled "Mobile Security and the Mobile Trusted Module"	Higher education	Inter-national	100	RHUL
09/2008	Outpost 24 Security Conference	Professionals	Inter-national	100	ISE
8/10/2008	SecTor Security Conference	Security Professionals	Canada, USA	100	ISE
21/10/ - 24/10/2008	Systems 2008: Industry fair - Embedded Trusted Computing for increased security and safety in Munich, Germany	Developers	Inter-national	~200	IFX
10/2008	Keynote at the Asia Pacific Trusted Computing Conference (APTC 2008)	Higher education, industry	Inter-national, SE Asia	250	HP
10/2008	IBM Innovation Center Showcase	IBM Partners in Turkey	National, Turkey	50	PORT
11/2008	Professional course "Introduction to Trusted Computing"	Industry	National, Italy	~20	POL
11/2008	IST Event 2008	Higher education, industry, public	Europe	N/A	POL, TUB, HP, BME
11/2008	Talk	TC Experts	Inter-national	N/A	IAIK
25/11-27/11/2008	ICT 2008 conference http://ec.europa.eu/information_society/events/ict/2008/index_en.htm	Higher education, industry	Europe	~4000	TEC, HP, ITAS, POL, IAIK
28/11/2008	AXMEDIS Conference 2008 Panel for Issues in security for Digital Rights Management	Scientific community, research	Inter-national	40	LDV
05/12-10/12/2008	SOSP 2008 http://www.sosp.org/	Higher education, industry	Inter-national	~500	TUD
08/12-	OSDI 2008,	Higher	Inter-	~500	TUD

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
10/12/2008	http://www.usenix.org/events/osdi08/	education, industry	national		
12/2008	Workshop "Betriebssystemsicherheit"	Industry, academia, law enforcement	National, Germany	100	HP
Spring 2008	Elective course on trusted computing in University of Kocaeli	Students	National, Turkey	25	TUB
2008	11 week MSc course in Trusted Computing.	Higher education	Inter-national	20	RHUL
2008	Conference paper on Functional Programming, "Hashconsing in an incre-mentally garbage-collected system:a story of weak pointers andhashconsing in ocaml 3.10.2", Pascal Cuoq	N/A	Inter-national, Canada	N/A	CEA
2008	Automotive TC workshop: Trusted computing for next generation of reliable automotive electronics	Automotive development experts, newcomers for trusted computing	Inter-national	~ 200	IFX
2008	Mobile phone workshops: Trusted computing as integrated part of mobile phones	Mobile phone development experts	Inter-national	~ 200	IFX
2008	Trusted Computing Summer School 2008 and following one week event: Training and discussion for students and interested researchers	Higher education	Inter-national	~40	IFX
2008	Presentation at Airbus Workshop Toulouse	Avionics	Europe	50	CEA
04/2009	Papers and Talks	TC Experts	Inter-national	80	IAIK
24/02/2009	Talk: "Satori: Enlightened page sharing." Xen Summit, San Francisco, CA	Industry	Inter-national	N/A	CUCL
24/02/2009	Talk: "Flexible and secure hardware 3D rendering on Xen." Xen Summit, San Francisco, CA	Industry	Inter-national	N/A	CUCL

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
05/03/2009	Tutorial on the trusted mobile platform at University of Bristol	Higher education	Inter-national	10	RHUL
19/03/2009	Lecture on Trusted Computing for MSc in Information Security – Software security course	Higher education	Inter-national	30	RHUL
31/03/2009	Frama-C training session	Higher education, Industry	Europe	37	CEA
31/03/2009	Talk: "Secure 3D Graphics for Virtual Machines", EuroSec 2009 workshop, Nuremberg, Germany.	Higher education	Inter-national	40	CUCL
03/2009	Practical Lab for Master Course on TC at Royal Holloway University London	Higher education	Europe	~10	POL, RHUL
04/2009	Elective course on trusted computing in University of Kocaeli	Students	National, Turkey	25	TUB
01/04-03/04/2009	A paper was presented at the 17th International Workshop on Security Protocols, Cambridge, UK entitled "A novel stateless authentication protocol".	Higher education	Europe	40	RHUL
06/04-08/04/2009	A paper was presented at Trust 2009, Oxford, U.K., titled "A Property-dependent Agent Transfer Protocol"	Research	Europe	N/A	RHUL
05/2009	Knowledge Transfer Network IT Security	Higher education, Industry	National, UK	100	HP
06/2009	Professional course "Introduction t"	Industry	National, Italy	~20	POL
06/2009	Summer School at Carnegie Mellow University	Academia	Inter-national USA	~100	POL, HP
09/2009	Conference	ICT	Bulgaria, Greece, Romania	~300	TUS
09/2009	4rd European Summer School on Trusted Infrastructure	Higher education,	Europe	~100	POL and other

Planned/ actual dates	Type	Type of audience	Countries addressed	Size of audience	Partner (s)
	(ETISS) – Graz, Austria	Industry, TCG member			OpenTC partners
11/2009	2008 International Symposium on Trusted Computing	Scientific Conference	Inter-national	N/A	IAIK
11/2009	SITIS 2009: 5th international conference on signal-image technology & internet based systems	Higher education	Europe	400	TUB
2009	11 week MSc course in Trusted Computing	Higher education	Inter-national	10	RHUL
regularly	ISECOM Subscriber discussions	Professionals	Inter-national	1.000	ISE
regularly	News List	Professionals	Inter-national	30.000	ISE
regularly	ISECOM Subscriber discussions	Professionals	Inter-national	1.000	ISE
regularly	Penetration Testing Mailing List	Professionals	Inter-national	50.000	ISE
regularly	BugTraq Mailing List	Professionals	Inter-national	100.000	ISE
regularly	XEN Summit: AMD is a regular attendee of the XEN summit, which happens 2 to 4 times a year. AMD presents there new developments in virtualization and related security technologies	Higher education, Industry, Government	Inter-national	>100	AMD, HP, IBM
regularly	Distribution of the OpenTC newsletters	Industry, government, higher education, research	Inter-national	~300	TEC

Table 3: Detailed listing of dissemination activities

2.3 Description of major activities

2.3.1 1st European Trusted Infrastructure Summer School (2006)

The First European Summer School on Trusted Infrastructure was held on 3rd-8th September 2006 in Oxford, UK. The goal of the event was to bring together academics, researchers and advanced students to spend a week learning about

current developments in Trusted Computing and related technologies, and to explore the surrounding research agenda.

The programme included three key components: a series of lectures and practical classes on emerging trusted infrastructure technologies such as Trusted Computing, operating system and virtualization, running research discussions throughout the week and a number of keynote talks.

2.3.2 Grazer Linux Tag (2007)

The Linux days event series is a yearly workshop in different cities of Austria where people meet up to discuss and showcase new developments in IT areas, with special emphasis on open source software (OSS).

IAIK used this opportunity to present the fundamental workings of Trusted Computing technology and compare facts with the hyped mainstream media coverage. Through showcasing of available open source software packages for Trusted Computing for the Linux OS - including the packages developed and published by IAIK within OpenTC - the audience was encouraged to gain hands-on experience with Trusted Computing themselves.

2.3.3 The Second ACM Workshop on Scalable Trusted Computing (2007)

At the Workshop on Scalable Trusted Computing (STC'07) in 2007, OpenTC was well represented by IAIK and RUB. IAIK presented a paper about enhancing mobile and embedded devices with Trusted Computing (TC) technology. The presented work combines all software components required for accessing an MTM and shows how TC functionality can be provided for mobile applications. For the design of the new architecture, special attention was turned to reusing currently existing technology and hardware rather than designing new hardware. RUB gave three presentations titled “Reconfigurable Trusted Computing in Hardware”, “Beyond secure channels” and “Realising property-based attestation and sealing with commonly available hard- and software”. All presentations received much attention and response from the audience and made participants aware of the good work done within OpenTC.

2.3.4 European Conference on Security Research (2007)

SRC '07 was organised in the context of Germany's presidency of the EC council by the Federal Ministry for Education and Research in cooperation with the EC, DG Enterprise. The conference had invited high-level international speakers presenting on the current status of security research in the European Union.

SRC '07 covered presentation of far-reaching concepts, ideas and research programmes of the European Union. The conference was the launch event for the "European Security Research Programme", published for the first time as a separate programme under the 7th Research Framework Programme 2007-2013. This programme was geared towards improving the security of citizens in Europe, recognising the causes for threats to civil security, identifying effective

countermeasures and strengthening the competitiveness of Europe.

Further information: http://www.src07.de/

2.3.5 First Asia Pacific Trusted Infrastructure Summer School (2007)

The 1st Asia-Pacific Summer School on Trusted Infrastructure Technologies (APTISS'07) was held during the week of August 20-24, at the International Conference Center Hotel, City of ZhuHai, GuangDong Province, China.

Altogether 100 people participated, including 64 fully sponsored graduate school students from universities and academic institutes all over China researching in related areas. The School organised a program of 15 lectures provided by world renowned academic researchers in the area, expert architects from the standard specification body - Trusted Computing Group, and the industry's leading developers. It was reckoned by all participants including lecturers that the program had a cross-spectrum coverage of topics. In particular, Dirk Kuhlmann presented an in depth description of the OpenTC work from its design goals and motivation, through detailed descriptions of some of the technical approaches. The conference was extremely successful and there is a plan to hold a second school in 2008 where we expect to be able to present some of the results of OpenTC.

The conference covered the basics of TCG technology as well as trusted infrastructure developments as they relate to virtualisation technology, grid computing, and networking architectures. APTISS '07 complemented similar events in Europe (Oxford 2006, Bochum 2007).

Further information: http://www.aptiss.org/

2.3.6 Conference/Workshop "ACM CCS / STC 2006"

The workshop "Scalable Trusted Computing" (STC) is organised by the ACM, and co-located with the "Computer and Communications Security" (CCS) conference, one of the major security conferences worldwide. In 2006, STC took place for the first time. Due to its success, a second STC workshop was organised in 2007 (again together with CCS).

At STC, current research from various topics in the area of Trusted Computing with a particular focus on scalability were presented. RUB presented a research paper on property-based attestation, which is a line of research with special importance for scalability. We proposed an efficient cryptographic protocol for property-based attestation, following a delegation-based approach with a certificate issuer who - after issuing the certificates - can remain offline during all the protocols.

Another research paper presented by RUB was on testing TPMs for compliance with the TCG specifications. Systematic testing various TPM chips from different manufacturers revealed that many of them actually did not comply with the specifications. With the presentation and publication of these papers, RUB was able to disseminate results from the OpenTC project to a broad audience. Moreover, we got in contact with international top researchers, both from the area of Trusted Computing,

and from other fields of computer and communications security.

Attending the workshop and the conference led to a significant amount of fruitful discussions with security researchers from all over the world.

2.3.7 Workshop "WATC"

The "Second Workshop on Advances in Trusted Computing" (WATC), at Tokyo, Japan, was sponsored by the Ministry of Economy, Trade and Industry, Japan (METI) under contract, New-generation Information Security R&D Program.

The aim of WATC is to bring together scientists from the area of Trusted Computing, who present and discuss current research results.

IBM and RUB presented joint work: "Enhancing Grid Security Using Trusted Virtualisation". This paper described how a virtualisation-based architecture supporting Trusted Computing can be used to improve grid security. An example for such a system is the architecture currently developed within the OpenTC project.

RUB presented another paper: "Play it once again, Sam - Enforcing Stateful Licenses on Open Platforms". It showed how stateful licenses can be enforced based on Trusted Computing and virtualisation technology.

Moreover, Prof. Ahmad-Reza Sadeghi gave an invited talk "Trusting Trust - The Need and Challenges for Trusted Computing", where he presented our current research in Trusted Computing, including the OpenTC project. A further topic of this talk were the various challenges that have to be addressed before Trusted Computing can be rolled out on a large scale and in security critical contexts.

WATC was very successful in bringing together researchers and practitioners to discuss research issues and experience in the boundary areas between Trusted Computing and Information Security. A lot of interesting discussions with many experts and specialists in the field emerged, and RUB got in contact with other international top researchers.

2.3.8 2nd European Trusted Infrastructure Summer School (ETISS)

The Second European Trusted Infrastructure Summer School (ETISS) was organised by the University of Bochum (RUB) and kept a large audience of about 80 people very busy during an entire week. As for previous year's edition of the Summer School, TCG members from the industry (HP, IBM, Intel, AMD) gave presentations, as well as governmental bodies (the German's BSI and BMWi, the UK's CESG, and the French's DCSSI).

ETISS was the occasion to discover the latest developments in Trusted Computing, from Intel's TXT white list to the Mobile Trusted Module. A considerable amount of presentations were given, including topics not presented at last year's Summer School, such as Random Number Generators and the Storage specification.

This year, the research workshops discussed a lot of advanced topics, such as Trusted Computing protocols, the mobile platform and hardware attacks, and presented

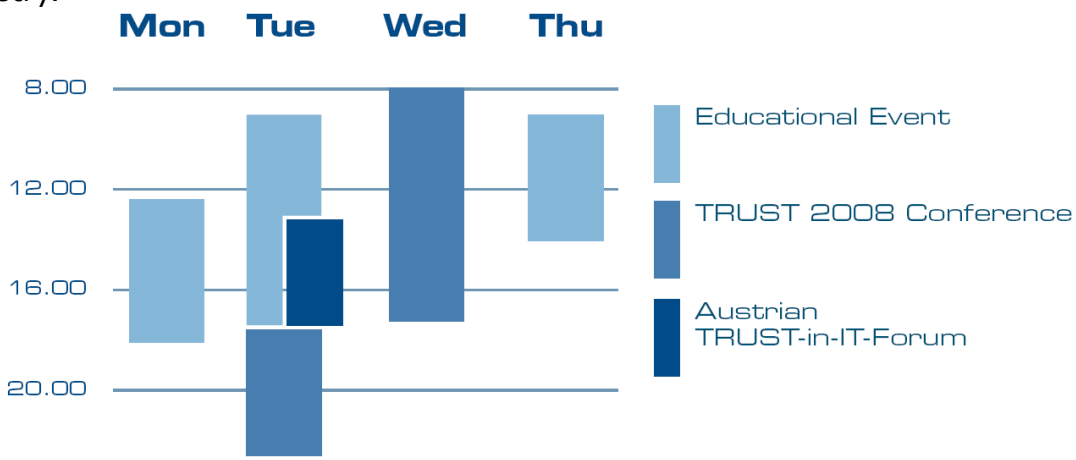
numerous promising results.

The OpenTC project was largely represented by a number of participants and speakers. The first proof-of-concept prototype was used during the practical assignments to introduce the notions of Trusted Computing (notably the TPM commands) and trusted virtualisation.

ETISS was a highly successful event, due to the high variety of content which included presentations of the latest ideas and implementation results, as well as discussions about the open questions in the field.

2.3.9 TRUST2008 Conference and Spring School

The most prominent dissemination event held in relation to the OpenTC project was TRUST2008, organised by Technikon. Trust2008 was an international event, which took place in Villach, Austria in March 2008 and brought together scientific stakeholders from all over the world in the field of trusted computing. The conference focused on trusted computing and trust in IT, and saw the presentation of both state of the art technologies and forward looking research papers. The main module, i.e. the scientific conference, served to maximise communication and knowledge exchange between international parties from both the scientific/research community and industry.



Picture 1: Time Planning for the TRUST2008 conference

During Trust2008, several project meetings and workshops took place. In the foreground was the OpenTC meeting, at which almost all partners were represented. The research papers presented during the scientific module at the conference (which are highly relevant to the work being completed within OpenTC) were published by Springer Verlag in LNCS 4968. Feedback indicated that the international audience from both industry and science was pleased by the mix of conference articles, project presentations and discussions. In total 159 participants (made up of people of 18 different nationalities from 4 continents) registered for Trust2008. It was the perfect occasion to present the state-of-the-art and beyond. Visions and possibilities for the future development were given as well as communication between science and industry was provided. Trust2008 fostered the knowledge exchange at the best possible rate.

2.3.10 ICT-Mobile Summit 2008

The ICT Mobile and Wireless Communications Summit took place in Stockholm. This was the seventeenth in a series of Annual Conferences supported by the European Commission, which regularly attract over 600 delegates from industry and research to share experiences and research results, identify future trends, discuss business opportunities and identify opportunities for international research collaboration under the ICT Theme FP7.

2.3.11 3rd European Trusted Infrastructure Summer School (ETISS)

The Third European Trusted Infrastructure Summer School was held in Oxford, 31st August - 5th September 2008. The venue was the Oriel College.

The aim of the summer school was to provide a programme which is attractive to masters' and doctoral students learning about Trusted Infrastructure for the first time, and also for academics and researchers with more experience. The event included introductory and more advanced lectures, practical labs, and research seminars. Many of those who have been instrumental in shaping the emerging Trusted technologies were among the lecturers, like David Grawrock, Graeme Proudler (HP Labs), Paul Congdon (HP ProCurve CTO), Robert Thibadeau (Seagate Chief Technologist), Paul England (Microsoft) and many others.

2.3.12 OpenTC newsletter

This service is designed to inform the interested public about downloadable prototypes, project achievements and other up-to-date information, and it is meant to support discussion about the underlying issues. We aim to publish this newsletter irregularly during the course of the project and beyond.

2.4 Articles in journals and magazines, papers and electronic publications

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
Since 2004	Information on Trusted Computing at: www.infineon.com/TPM	Developers, engineers, system integrators	Inter-national	IFX
24/02/2006 and 01/03/2006	Analysis and discussion of TC, and presentation of Open_TC views (Indicare Monitor)	Industry	N/A	LDV, HP, ITAS, TUM
14/11-17/11/2006	*SDR Technical Conference 2006 – Invited paper:* E. M. Gallery, C. J. Mitchell: "Trusted Computing Techno-logies and their	Research, industry	Inter-national	RHUL

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
	use in the Provision of High Assurance SDR Platforms"			
11/01/2007	IEEE CCNC '07 Conference (DRM Workshop) paper. Title: Efficient design of interpretation of REL license using Expert Systems	Scientific community, R&D personnel	Inter-national	LDV
02/2007	*European eChallenges e-2007 Conference & Exhibition* - Submitted paper	Industry, government, higher education	Europe	HP
02/2007	Magazine Paper	Higher education, public	Inter-national	CUCL
04/2007	Launch of new public website: www.opentc.net	Public	Inter-national	TEC
21/05-23/05/2007	*UbiSafe 2007, Ontario, Canada – paper:* E. Gallery, S. Balfe: "Mobile Agents and the Deus Ex Machina"	Higher education, research	Inter-national	RHUL
07/2007	Overview article in ENISA quarterly	Policy and technical experts	Europe	IAIK
07/2007 and 10/2007	First issues of the OpenTC project newsletter	Public	Inter-national	ITAS, TEC, HP, RHUL, All
08/08/2007	*Usenix Security 2007:* "OSLO paper"	N/A	N/A	TUD
08/2007	*Towards Automated Provisioning of Secure Virtualized Networks. S. Cabuk, C. Dalton, H. V. Ramasamy, and M. Schunter. Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS-2007)*	Scientific	Inter-national	IBM, HP
09/09 - 15/09/2007	E. M. Gallery, C. J. Mitchell: "Trusted Mobile Platforms". *In: A. Aldini, R. Gorrieri (eds.): FOSAD 2006/2007 - Tutorial Lectures. LNCS 4677, Springer-Verlag 2007, pgs 282-323*	Research	Inter-national	RHUL
27/09/2007	*1st International Workshop on Run*	Research	Germany	KUL

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
	Time Enforcement for Mobile and Distributed Systems (REM 2007): D. Schellekens, B. Wyseur, B. Preneel: "Remote attestation on legacy operating systems with trusted platform modules"			
16/10/2007	Article in Design & Elektronik: Trusted Hardware	TC- experts	Germany, Europe	IFX
11/2007	Journal article in 'Hiradastechnika'	IT and Comm. engineers	Hungary	BME
02/11/2007	T. Eisenbarth, T. Güneysu, C. Paar, A.-R. Sadeghi, D. Schellekens, M. Wolf: "Reconfigurable Trusted Computing in Hardware". *In: 2nd ACM Workshop on Scalable Trusted Computing (STC 2007), ACM Press, pp. 15-20, 2007*	Research	US	RUB, KUL
12/2007	Chapter in a Teletrust book: "Trusted Computing Introduction"	TC- experts, students	German-speakers	IFX
2007	Paper on the C code static analysis tool	Industry	Inter-national	CEA
2007	Publication	Researchers, industry	Inter-national	CEA
2007	Publication on CEA intranet	Employees of CEA	CEA	CEA
2007	Publication	Industry	National	CEA
2007	Presentation	Internal: laboratories, department and company meetings	CEA	CEA
Since 2007	General trusted computing news site (trustedforum.org)	Public	Inter-national	TUB
01/2008	*SOFSEM 2008* Invited Talk, LNCS 4910, 2008 "Trusted Computing—State of the Art and Challenges."	Research	Inter-national	RUB
18/01/2008	*1st COMMUNIA International Workshop on Technology and the Public Domain, Torino, Italy:*A. Lioy, G. Ramunno, D. Vernizzi: "Trusted Computing and Infrastructure Commons"	Higher education, research, government	Europe	POL
03/2008	*TRUST2008* - Conference paper	Research	Austria	CEA

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
03/2008	B. Jansen, H.G.V. Ramasamy, M. Schunter: "On Integrity Protection and Verification for Virtual Machines" In: Proceedings of the 4th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments 2008 (VEE '08), Seattle, pgs. 101-110	Higher education, industry	Inter-national	IBM
07/03/2008	*ACM VEE 2008 - Scientific paper:* "Improving Xen security through disaggregation"	Higher education	Inter-national	CUCL
10/03-14/03/2008	*Trust 2008, Villach, Austria. – Scientific paper:*A. Leung, L. Chen, C.J. Mitchell: "On a possible privacy flaw in Direct Anonymous Attestation (DAA)" (http://www.trust2008.eu/)	Research	Europe	RHUL
10/03-14/03/2008	An invited talk was presented at the TRUST2008 educational event titled "Who is the TCG and What are the TCG Concepts?".	Higher education	Europe	RHUL
10/03 - 13/03/2008	Klaus Kursawe and Dries Schellekens, "Flexible µTPMs through Disembedding," In *Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security*	Higher education	Inter-national, Australia	KUL
12/03/2008	Dries Schellekens, Pim Tuyls and Bart Preneel, "Embedded Trusted Computing with Authenticated Non-Volatile Memory," In *1st International Conference on Trusted Computing and Trust in Information Technologies (TRUST 2008) and In: K. Koch, P. Lipp, and A. Sadeghi (eds.): TRUST 2008. LNCS 4968, Springer-Verlag, 2008, pgs. 60-74*	Higher education	Inter-national	KUL
12/03/2008	*Trust 2008, Villach, Austria. – Scientific paper:* C. Weinhold, H. Härtig: "Trusted Computing Serving an Anonymity Service"	Higher education, industry, government	Inter-national	TUD
31/03/2008	E. Cesena, G. Ramunno, D. Vernizzi: "Secure storage using a sealing proxy". *In: Proceedings of the ACM SIGOPS European Workshop on System Security*	Higher education, research,	Europe	POL, CUCL

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
31/03/2008	*EuroSec 2008 - Scientific paper: "Privilege separation made easy"*	Higher education	Inter-national	CUCL
31/03-04/05/2008	A. Böttcher, B. Kauer, H.Härtig: "VPFS: Building a Virtual Private File System with a Small Trusted Computing Base". *Proceedings of the EuroSys 2008 Conference*	Higher education, industry	Inter-national	TUD
04/2008	*The 4th Information Security Practice and Experience Conference (ISPEC 2008), Sydney, Australia. - scientific paper:"Securing Peer-to-peer Distributions for Mobile Devices"*	Research	Inter-national	RUB
04/2008	S. Balfe, E. Gallery, C. J. Mitchell, K. G. Paterson: "Crimeware and Trusted Computing". *In: M. Jakobsson, Z. Ramzan (eds.): Crimeware. Understanding New Attacks and Defenses. Addison-Wesley*	Industry, research	Inter-national	RHUL
04/2008	A proposal for a book on Trusted computing and its applications has been accepted by Cambridge University Press	Industry, higher education, research	Inter-national	RHUL
05/2008	Cabuk, S.; Dalton, C. I.; Ramasamy, H. V.; Schunter, M. Declarative Security Specification of Virtual Networks. *The Rise and Rise of the Declarative Datacenter*. R2D2 Workshop, Microsoft Research,	Higher education, research	Inter-national	IBM, HP
15/05/2008	S. Cabuk, C.I. Dalton, K. Eriksson, D. Kuhlmann, H. Govind, V. Ramasamy, G. Ramunno, A.R. Sadeghi, M. Schunter, C. Stueble: "Towards Automated Security Policy Enforcement in Multi-Tenant Virtual Data Centers". *Submitted to Journal of Computer Security (JCS) for 6th FP European Projects*	Higher education, research	Europe	HP, IBM, POL, RUB
19/05-22/05/2008	*3rd International Workshop on Workflow Systems in e-Science 2008, Lyon, France:* P.W. Yau, A. Tomlinson, S. Balfe and E. Gallery: "Securing Grid Workflows with Trusted Computing (Extended Abstract)"	Research	Europe	RHUL
06/2008	*ACM CCS STC'08*:Paper about Trusted Channels submitted	Research, professionals	Inter-national	RUB, POL

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
06/2008	*ACM CCS STC'08*:Paper about building Trusted Computing applications	Research, professionals	Inter-national	POL
06/2008	*ACM CCS STC'08*: Cabuk, S.; Grete, P.; Plaquin, D. Towards Virtual Platforms	Research, Scientific	Inter-national	HP
06/2008	*IEEE TrustCom2008:* Paper about Trusted Broadcast Encryption	Research	Europe	POL
06/2008	Paper	Technical Experts	Inter-national	IAIK
21/06/2008	Cabuk, S.; Plaquin, D.; Hong, T.; Murray, D.; John, E. Improving Policy Verification Capabilities of Trusted Platforms, HP Labs technical report HPL-2008-71	Research, Scientific	Inter-national	CUCL, HP
23/06-25/06/2008	*ICCS 2008 - 8th International Conference on Computational Science, Krakow, Poland:* P.W. Yau, A. Tomlinson, S. Balfe, E. Gallery: "Securing Grid Workflows with Trusted Computing"	Research	Inter-national	RHUL
08/2008	B. Jansen, H.G.V. Ramasamy, M. Schunter, A. Tanner: "Architecting Dependable and Secure Systems using Visualization" *In: R. d. Lemos, F. Di Giandomenico, C. Gacek, H. Muccini, M. Vieira (eds.): "Architecting Dependable Systems V". Berlin: Springer LNCScience 5135*	Higher education, industry	Inter-national	IBM
09/2008	The new new thieves	Professionals	Inter-national	ISE
09/2008	S. Balfe, E. Gallery, K. Paterson and C.J. Mitchell, "Challenges for trusted computing", IEEE Security and Privacy, volume 6, number 6, pgs 60-66, November/December 2008.	Industry, Higher education, Research	Inter-national	RHUL
08/09-10/09/2008	*IAS 2008 - 4th International Conference on Information Assurance and Security, Naples, Italy:* A. Leung, C.J. Mitchell: "A Device Management Framework for Secure Ubiquitous Services Delivery"	Research	Inter-national	RHUL
23/10-24/10/2008	"Trusted-Computing Technologies for the Protection of Critical Information Systems" A. Lioy, G. Ramunno, D.	Higher education, research,	Inter-national	POL

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
	Vernizzi*(CISIS'08 - Int. Workshop on Computational Intelligence in Security for Information Systems)*	industry		
31/10/2008	"An Efficient Implementation of Trusted Channels Based on OpenSSL" F.Armknecht, Y.Gasmi, A.R.Sadeghi; P.Stewin, M.Unger, G.Ramunno, D.Vernizzi *(STC'08: 3rd ACM workshop on Scalable Trusted Computing 2008)*	Higher education, research	Inter-national, US	RUB, POL
31/10/2008	"Boxing clever with IOMMUS" VMSec, Fairfax, VA	N/A	Inter-national	CUCL
11/2008	Talk	TC Experts	Inter-national	IAIK
18/11-20/11/2008	*"Towards Trusted Broadcast Encryption" E.Cesena, G.Ramunno, D.Vernizzi (TrustCom 2008: The 2008 International Symposium on Trusted Computing*)	Higher education, research	Inter-national, China	POL
2008	E. Gallery, C.J. Mitchell: "Trusted Computing: Security and Applications", *In: Cryptologia. Taylor & Francis*	Research	Inter-national	RHUL
2008	*K. Koch, P. Lipp, and A.R. Sadeghi (eds.): TRUST 2008. LNCS 4968, Springer-Verlag, 2008,*	Research	Inter-national	TEC, IAIK, RUB
2008	*ASIACCS'08 – scientific paper:* "Provably Secure Browser-Based User-Aware Mutual Authentication over TLS	Research	Inter-national	RUB
2008	*CHES 2008 – accepted paper:* "Efficient Helper Data Key Extractor on FPGAs"	Research	Inter-national	RUB
2008	A.R. Sadeghi, C. Stüble, M. Winandy: "Property-Based TPM Virtualization." *Proceedings of 11th Information Security Conference (ISC 2008)*	Research	Inter-national	RUB
2008	"A Demonstrative Ad-hoc Attestation System." *Proceedings of 11th Information Security Conference (ISC2008)*	Research	Inter-national	RUB
2008	L. Chen, H. Löhr, M. Manulis, A.R. Sadeghi: "Property-Based Attestation without a Trusted Third Party."	Research	Inter-national	RUB

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
	Proceedings of 11th Information Security Conferene (ISC 2008)			
2008	"Resettable and Non Transferable Chip Authen-tication for E-Passports." *RFIDSec 2008*	Research	Inter-national	RUB
2008	"User Privacy in Transport Systems Based on RFID E-Tickets." *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications (PiLBA)*	Research	Inter-national	RUB
2008	"An Efficient Implementation of Trusted Channels based on OpenSSL." *Proceedings of ACM STC'08*	Research	Inter-national	RUB
2008	"Flexible and Secure Enterprise Rights Management based on Trusted Virtual Domains." *Proceedings of ACM STC'08*	Research	Inter-national	RUB
2008	D. Schellekens, P. Tuyls, B. Preneel, "Remote attestation on legacy operating systems with trusted platform modules.". In: F. Massacci, F. Piessens (eds.): Electronic Notes in Theoretical Computer Science. *Proceedings of the First International Workshop on Run Time Enforcement for Mobile and Distributed Systems (REM 2007). Vol 197(1), Elsevier, 2008, pgs. 59-72*	Higher education, TC-experts	Inter-national	KUL
2008	S. Cabuk, C.I. Dalton, K. Eriksson, D. Kuhlmann, H. Govind, V. Ramasamy, G. Ramunno, A.-R. Sadeghi, M. Schunter, C. Stüble: "Towards Automated Security Policy Enforcement in Multi-Tenant Virtual Data Centers" - *Submitted to Journal of Computer Security*	Higher education, industry	Inter-national	IBM, HP, RUB
2008	D. Schellekens, B. Wyseur, B. Preneel: "Embedded Trusted Computing with Authenticated Non-Volatile Memory". *In: K. Koch, P. Lipp, and A. Sadeghi (eds.): TRUST 2008. LNCS 4968, Springer-Verlag, 2008, pgs. 60-74*	N/A	N/A	KUL
2008	Contribution to project newsletter	TC-experts	Inter-national	ITAS, RHUL, TEC, HP

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
2008	Paper on the C code static analysis tool	Industry	Inter-national	CEA
2008	Product web site http://frama-c.cea.fr	Public	Inter-national	CEA
2008	Trustworthy Global Computing, Revised Selected Papers	Public	Inter-national	IAIK
2008	Proceedings of the 2008 International Symposium on Trusted Computing, TrustCom 2008	Public	Inter-national	IAIK
01/2009	SIGOPS Journal on Operating Systems	Higher education, industry	Inter-national	HP
01/2009	"Towards Automated Security Policy Enforcement in Multi-Tenant Virtual Data Centers" Serdar Cabuk, Chris I. Dalton, Konrad Eriksson, Dirk Kuhlmann, Hari Govind V. Ramasamy,Gianluca Ramunno, Ahmad-Reza Sadeghi, Matthias Schunter and Christian Stueble *(accepted for the special issue of Journal of Computer Security, JCS) for 6th FP European Projects)*	Higher education, research	Europe	HP, IBM, POL, RUB
02/2009	Trusted Computing (book chapter for Springer & Verlag)	Public	Inter-national	POL
03/2009	"Towards Automated Security Policy Enforcement in Multi-Tenant Virtual Data Centers" Serdar Cabuk, Chris I. Dalton, Konrad Eriksson, Dirk Kuhlmann, HariGovind V. Ramasamy, Gianluca Ramunno, Ahmad-Reza Sadeghi, Matthias Schunter and Christian Stueble *(accepted for the special issue of Journal of Computer Security, JCS) for 6th FP European Projects)*	Academia, Research	Europe	HP, IBM, POL, RUB
31/03/2009	Workshop paper: Adam Lackorzynski, Alexander Warg, "Taming Subsystems: Capabilities as Universal Resource Access Control in L4", IIES 2009: *Workshop on Isolation and Integration in Embedded Systems, Nuremberg*	Higher education, Industry	Inter-national	TUD
31/03/2009	Workshop paper: Michael Peter,	Higher	Inter-	TUD

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
	Henning Schild, Adam Lackorzynski, Alexander Warg, "Virtual Machines Jailed", *VTDS'09: EuroSys Workshop on Virtualization Technology for Dependable Systems, Nuremberg*	education, Industry	national	
04/2009	Papers and Talks	TC Experts	Inter-national	IAIK
04/2009	Dirk Weber, Arnd Weber, Stephane Lo Presti: Requirements and Design Guidelines for a Trusted Hypervisor User Interface in: Proceedings of Future of Trust in Computing Conference, Berlin, 2008. 2009	N/A	Inter-national	ITAS, RHUL
04/2009	E. Gallery, A. Nagarajan and V. Varadharajan, "A property dependent agent transfer protocol", in: *Proceedings of Trust 2009, L. Chen, C. J. Mitchell and A Martin (eds.), LNCS 5471, Springer-Verlag, 2009, pp.240-264.*	Research	Inter-national	RHUL
05/2009	Paper about Trusted Migration *(Crisis 2009?)*	N/A	N/A	POL
06/2009	Paper about WYSIWYS *(ACM STC'09?)*	N/A	N/A	POL
06/2009	Paper about DAA-enhanced TLS *(ACM STC'09?)*	N/A	N/A	POL
07/07 - 10/07/2009	International Course on State of the Art and Evolution of Computer Security and Industrial Cryptography 2009	Academia, Industry, Government	Leuven, Belgium	KUL
11/2009	S. Balfe, E. Gallery, K.Paterson and C.J. Mitchell, "Challenges for Trusted Computing," *IEEE Security and Privacy, vol. 6, no. 6, p. 60ff*	Industry, Higher education, Research	Inter-national	RHUL
To appear 2009	A Secure Wallet for a Mobile Trusted Platform; OpenTC newsletter; E. Delfs, D. E. Gallery, D. Jennings, H. Loehr	General public	Inter-national	RHUL, RUB, IFX
To appear 2009	General trusted computing news site (trustedforum.org)	Public	Inter-national	TUB
To appear 2009	A. Leung, P.W. Yau, C.J. Mitchell: "Using Trusted Computing to Secure Mobile Ubiquitous Environments". *In: S. Gritzalis, T. Karygiannis, C.*	Research	Inter-national	RHUL

Planned/ actual dates	Type	Type of audience	Countries addresses	Partner (s)
	Skianis (eds.): Security and Privacy in Wireless and Mobile Networking. Troubador Publishing			
To appear - 2009	E. Gallery and C.J. Mitchell, "Trusted Computing: Security and Applications", *Cryptologia (a quarterly journal devoted to all aspects of cryptology) published by Taylor & Francis*	Research	Inter-national	RHUL
To appear 2009	"Modeling Trusted Computing Support in a Protection Profile for High Assurance Security Kernels." *Accepted for TRUST 2009*	Research	Inter-national	RHUL
To appear 2009	"Secure VPNs for Trusted Computing Environments." *Accepted for TRUST 2009*	Research	Inter-national	RHUL
To appear 2009	"Trusted Privacy Domains — Challenges for Trusted Com-puting in Privacy-Protecting Information Sharing". *Accepted for Information Se-curity Practice and Experience Conference (ISPEC'09)*	Research	Inter-national	RHUL
To appear 2009	EEE Multimedia Magazine, "The Open Access Application Format"	Research	Inter-national	LDV
In preparation	Paper about building Trusted Computing applications	N/A	N/A	POL
In preparation	Paper about Trusted Virtual Domains (TVDs) Policies	Research	N/A	POL, other OTC partners
Review pending	Journal article	Professionals	Hungary	BME
To appear 2010	Paper about KMA *(ACM Eurosys '10?)*	N/A	N/A	POL

Table 4: Publications

3 Section 3 – Publishable results

To enable maximum community benefit, the project results were integrated into, and distributed as, Open Source software, supporting Linux in particular. A main objective was the development of complete trusted Linux kernels for different use classes, which will be distributed as part of the Novell/SUSE (a project member) Linux distribution package. By making the project results widely available, the OpenTC consortium expects to encourage Europe's IT industry to invest in trust and security development. Especially small and medium-sized enterprises, industry, and research institutions will be enabled to develop and market trusted computing systems and applications independently. The integration of trust and security into next-generation European products will make these more competitive on the world market.

An important result achieved during the second period of the project was the publication of its first prototype for Privacy Enhanced Transactions (PET). It was released as proof-of-concept because it was an intermediate step towards a more comprehensive solution, did not contain all components of the architecture and included components that were not in a finalised form. With a few minor exceptions, the source code was released under the GNU GPL version 2 license and provided as both a Live CD (binaries) and source code. It was tested on HP and IBM laptops equipped with Trusted Platform Modules (TPMs) and distributed with a disclaimer of responsibility.

In 2008 the second proof-of-concept prototype, the CC@HOME (Corporate Computing at Home) was developed. (it could also have been termed "Private Computing on Corporate Platforms".) It reflects the situation where employers tolerate, within reasonable limits, the utilization of corporate equipment (in particular notebooks) for private purposes. However, while conniving in the private use of their equipment, employers still want a safeguard that their machinery remains fit for being used on their corporate network. The prototype was capable of hosting both proprietary and non proprietary operating systems and came with a much improved graphical user interface that allowed simplified switching between compartments and roles. It was produced using SuSE's build environment and and disseminated under GPLv2 through SuSE's repositories that are mirrored worldwide. The prototype raised considerable interest in product divisons of industrial partners. An extended version has been used extensively as hands-on training system for Trusted Computing technology since 2007.

The third proof-of-concept prototype addresses a virtual datacenter scenario and will be released as dedicated OpenSuSE 11.1 distribution under GPLv2 in 2009. The system allows to create and manage mutually isolated "Trusted Virtual Domains", that is, clusters of virtual machines residing on arbitrary nodes of a managed infrastructure. The architecture provides for sophisticated logical isolation of data and management traffic. It includes platform components for network separation, tools for managing physical and virtual components, and a console implementation allowing to map Trusted Virtual domains to dedicated management compartments hosting the

administrative frontends. OpenTC results will also be included as improvements in upstream packages and will thereby become part of future distributions of Linux and Xen. Like the second proof-of-concept prototype, the third one will be extended and maintained as training system for academic and industrial use.

In addition to the proof-of-concept prototypes, all of OpenTC's documentation and courseware have been made publicly available under the Creative Commons license. Further details and publishable results can be found in the OpenTC webpage (www.opentc.net) in the Publications and download sections. Furthermore all released Newsletters can be read on the OpenTC webpage. This service was designed to inform the interested public about downloadable prototypes, project achievements and other up-to-date information, and it is meant to support discussion about the underlying issues.

Details and further publishable results can be found in the OpenTC webpage (www.opentc.net) in the Publications and download sections. Furthermore all released Newsletters can be read on the OpenTC webpage. This service was designed to inform the interested public about downloadable prototypes, project achievements and other up-to-date information, and it is meant to support discussion about the underlying issues.

4 Section 4 - Cooperation with external organisations

In addition to the various dissemination activities reported above, the OpenTC consortium was in close cooperation with external organisations during the whole project duration and also beyond it. The involved partners and their activities are listed below.

Planned/ actual Dates	Type	External organisation(s)	Countries addressed	Partners involved
01/2006-10/2006	Discussions, five 2-hour telephone conferences and a half-day meeting	Vodafone, TCG MPWG (Mobile Phone Work Group)	International	RHUL
01/2006-12/2007	Weekly 2-hour telephone conferences; discussions	Software Define Radio forum; SDR Security Working Group	International	RHUL
01/2006-10/2006	Discussions, 5 2-hour telephone conferences and a half-day meeting	Vodafone, TCG MPWG (Mobile Phone Work Group)	International	RHUL
02/2006-03/2006	Addition to the eMobility work plan, several emails between February and March 2006	European Commission, eMobility Group	N/A	IFX, RUB, TUD, RHUL
03/09-08/09/2006	European Summer School on Trusted Infrastructure technologies	Higher education	International	RHUL, RUB, HP, CUCL, TUD
01/11/2006	Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya and Mira Meyerovich, "How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication," In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006)*	Higher education	International	KUL, IBM
02/11/2006	OSLO+TC demonstration, Intel, Hillsboro, USA	Industry	International	TUD
16/11-17/11/2006 and 16/04-17/04/2007	Attendance of meetings of the security working group	SDR Forum	International	RHUL
11/2006 - 12/2007	Presentation of the Open Trusted Computing demonstrator system	Industry	National, UK	RHUL

Planned/ actual Dates	Type	External organisation(s)	Countries addressed	Partners involved
	at the Royal Holloway's HP Colloquium			
12/2006	Collaborative work, knowledge transfer	Dresden Silicon	National, Germany	TUD
2006-2010	Support IFX in reviewing interim OMTP specifications on hardware and application soft-ware security and requirements analysis documents. Check that WP8 OpenTC documents are consistent with OMTP specifications and proposals as they become available.	Industry, research	Inter-national	IFX / COM2
02/02/2007	Meeting of the Special Interest Group on Trusted Computing in the Cyber Security KTN (Knowledge Transfer Network) organised by the UK's DTI (Department of Trade and Industry)	Cyber Security Knowledge Transfer Network	National, UK	RHUL
14/03/2007	Collaborative work, knowledge transfer	Microsoft Redmond	N/A	TUD
20/03/2007	Collaborative work, knowledge transfer	CUCL Cambridge	N/A	TUD
30/03/2007	Collaborative work, knowledge transfer	Trialog+EADS	N/A	TUD
13/04/2007	Collaborative work, knowledge transfer	Telecom Labs	N/A	TUD
11/05/2007	Collaborative work, knowledge transfer	Microsoft, Aachen	N/A	TUD
18/05/2007	Collaborative work, knowledge transfer	Atsec	N/A	TUD
12/06/2007	Collaborative work, knowledge transfer	Intel, Budapest	N/A	TUD
07/2007-12/2007	Collaborative work, knowledge transfer	Macquarie University, Sydney, Australia	Inter-national	RHUL
19/07/2007	Collaborative work, knowledge transfer	AMD, Austin	Inter-national	TUD
23/07-29/07/2007	Collaborative work, knowledge transfer	National Research Council of Canada (NRC)	inter-national	RHUL

Planned/ actual Dates	Type	External organisation(s)	Countries addressed	Partners involved
30/07/2007	Collaborative work, knowledge transfer	MPI Saarbrücken	N/A	TUD
02/08/2007	Collaborative work, knowledge transfer	IBM Watson	N/A	TUD
14/08/2007	Collaborative work, knowledge transfer	CMU, Pittsburgh	N/A	TUD
27/08/2007	Collaborative work, knowledge transfer	Infineon	N/A	TUD
20/09/2007	Collaborative work, knowledge transfer	Motorola	N/A	TUD
27/09/2007	Dries Schellekens, Brecht Wyseur and Bart Preneel, "Remote attestation on legacy operating systems with trusted platform modules," In *1st International Workshop on Run Time Enforcement for Mobile and Distributed Systems (REM 2007)*	Higher education	National, Germany	KUL
09/2007-12/2007	Collaborative research visit from RHUL to Macquarie University, Sydney, Australia	Macquarie University, Sydney, Australia	Australia, UK	RHUL
29/09–05/10/2007	2nd European Summer School on Trusted Infrastructure – Bochum, Germany	Higher education, industry, TCG members	Europe	RUB, POL, HP, TUD, IFX
02/11/2007	Thomas Eisenbarth, Tim Güneysu, Christof Paar, Ahmad-Reza Sadeghi, Dries Schellekens, and Marko Wolf, "Reconfigurable Trusted Computing in Hardware," In *2nd ACM Workshop on Scalable Trusted Computing (STC 2007)*	Higher education	Alexandria, Virgina, USA	RUB, KUL
05/11/2007	Collaborative work, knowledge transfer	Vmware	N/A	TUD
11/11/2007	Collaborative work, knowledge transfer	Quimonda	N/A	TUD
2007	Collaborative work, knowledge transfer	Swedish Armed Forces	National, Sweden	IBM
09/2008	3rd European Summer School on Trusted Infrastructure (ETISS) – Oxford, UK	Higher education, industry, TCG member organizations	Inter-national, Europe	POL, other OpenTC partners
Q4 2008	Joint Research Project proposal	METU IAM	Turkey	PORT

Planned/ actual Dates	Type	External organisation(s)	Countries addressed	Partners involved
	on GRID security funded nationally by the Ministry of Industry			
Q4 2008	Joint research project proposal with IBM Turkey	IBM partners	Turkey	PORT
Q4 2008	Joint research project proposal with Ministry of Health on patient data privacy (but not necessarily trusted computing)	Ministry of Health, Turkey	Turkey	PORT
06/04-08/04/2009	Trust 2009 International Conference (programme co-chair)	Higher education, Research, Industrial researchers	Inter-national	RHUL, CUCL
09/2009	4th European Summer School on Trusted Infrastructure (ETISS) – Graz, Austria	Academia and Industry, TCG member organizations	Europe	PoI and many other OpenTC partner
Ongoing Cooperations				
Since 2004	Active participation in TCG standardisation and manage-ment meetings; bringing current TCG pre-standard activities early into the OpenTC work and activities	TCG (Trusted Computing Group)	Inter-national	IFX, HP, IBM,AMD, POL, IAIK
Since 2004	Information about Trusted Computing for embedded systems	Several mobile phone standardization organisations	Inter-national	IFX
Since 2006	Information about Trusted Computing for embedded systems	VDA Association of automotive industry	National, Germany	IFX
Since 01/2007	Cryptographic Research	Philips	N/A	RUB
Since 02/2007	Research on Trusted Channels	Nokia	N/A	RUB
Since 07/2007	Research on Trusted Computing for Embedded Devices	Philips, Intrinsic ID	N/A	KUL
Since 11/2007	Standardization within the Java Community Process (JCP) - JSR 321	Java Standardisation	Inter-national	IAIK, PORT, CUCL
Since 2007	Support IFX in taking part in	Industry, Research	Inter-	IFX, COM2

Planned/ actual Dates	Type	External organisation(s)	Countries addressed	Partners involved
	OMTP conference calls and meetings on hardware security, and check that the WP8 Open_TC documents are consistent with OMTP specifications and proposals as they become available		national	
Bi-weekly	Software Defined Radio (SDR) Forum conference calls	SDR Forum	N/A	RHUL
Ongoing	Distributed Management Task Force	Industrial	Inter-national	HP
Ongoing	MPEG Standardisation	Industry	Inter-national	LDV
Ongoing	Mutual information sharing, planning of possible dissemination activities	Developers	Turkey	PORT, TUB
Ongoing	Participating in the standardisation work of the Trusted Computing Group (TCG); bringing current TCG pre-standard activities early into the OpenTC work and activities	TCG	Inter-national	AMD, HP, IAIK, IBM, IFX, POL
Ongoing	The secure initialization (DRTM) prototype developed in OpenTC was used as the base of a standardization effort driven by AMD in the Trusted Computing Group (TCG). The specification will describe, how to build DRTM platforms all major existing platforms in a standardized way. The specification is expected to be released to the public later this year.	Industry, Government	Europe (mainly Germany, UK), USA	AMD, HP, IBM
Ongoing	Cooperation on developing secure 3D graphics virtualization	Tungsten Graphics	USA	CUCL
Ongoing	Cooperation on developing secure I/O virtualization	Intel, XenSource	UK	CUCL
Ongoing	Continued efforts to put the developed secure startup solution into a specification in the Trusted Computing Group	Novell, Government	UK, Germany, USA, ...	HP, IFX
Ongoing	Presentation and discussion of results and achievements	PhD students, industry	Inter-national	TUD

Planned/ actual Dates	Type	External organisation(s)	Countries addressed	Partners involved
Ongoing	Collaborative work, knowledge transfer	Nokia research, Finland	Inter-national	RUB
Ongoing	Collaborative work, knowledge transfer	Intel Corp., UK/US	Inter-national	RUB
Ongoing	Collaborative work, knowledge transfer	Philips, Netherlands	Inter-national	RUB
Ongoing	Collaborative work, knowledge transfer	University of Salerno, Italy	Inter-national	RUB
Ongoing	Collaborative work, knowledge transfer	University of Louvain la Neuve, Belgium	Inter-national	RUB
Ongoing	Collaborative work, knowledge transfer	Oxford University, UK	Inter-national	RUB
Ongoing	Collaborative work	Politecnico di Torino, Italy	Inter-national	RUB
In preparation	Support IFX with security expertise for mobile phone workshops: Security & Trusted computing as integrated part of mobile phones	Mobile phone developers	Inter-national	IFX

Table 5: Cooperation with external organisations

5 Section 5 - Participation in running / labelled projects

5.1 Participation in complementary EC projects

ITEA		
ES_PASS	Spread the use of static analysis techniques for the verification and validation of embedded software.	CEA
TECOM (ITEA)	*Trusted Embedded Computing* The strategic objective of TECOM is to investigate solutions and architectures for embedded systems platforms which need to meet both security and integrity requirements. The TECOM approach will be to apply the concept of trusted platforms to real-time embedded systems.	TUD, TEC

MEDEA		
TSC	The Trusted and Secured Computing (TSC) project aims at developing a family of HW/embedded SW silicon components enforcing secure and trusted computing in the Consumer, Computer, Telecommunications and Wireless areas. It also intends to develop and promote a family of relevant European standards while keeping inter-operability with existing US-led or Asian initiatives.	TEC

ICT FP7		
CACE	*The Computer Aided Cryptography Engineering* A EU-funded consortium of twelve partners, aims at developing a toolbox that supports the production of high quality cryptographic software. Development of hard-ware devices and software products is facilitated by a design flow, and a set of tools (e.g., compilers and de-buggers), which automate tasks normally performed by experienced, highly skilled developers. However, in both hardware and software examples the tools are generic since they seldom provide specific support for a particular domain.	TEC, RUB
ECRYPT II	*Network of Excellence in Cryptology–Phase II* Its aim is to ensure a durable integration of European research in both, academia and industry, and to maintain and strengthen the European excellence in these areas.	KUL, RHUL, IBM, RUB
€-confidential	*Trusted SW execution based on COTS* Trusted Security Platform to secure multi kind of application and to provide a trustworthy execution environment for sensitive applications (PMR, e-vote, e-bank, …) running on COTS.	CEA
eMuCo	*Embedded Multi-Core Processing for Mobile Communication Systems*	TUD via GWT

	The aim of the ICT-eMuCo project is to develop a platform for future mobile devices based on multi-core architecture. This comprises the relevant controller element as well as the operating system and application layers.	
MASTER	MASTER helps translate business level challenges to high-level challenges: - Decision Support to transform and aggregate lower level and scattered security information on a complex web of services to a level that is amenable to board room action based on concrete information, based on key security indicators. -A trusted Monitoring Infrastructure of the business SOA and outsourced infrastructure to provide the real-time information on the actual security status of the system at different level of granularity. -An Infrastructure for Enforcement of the security and trust decisions from the board level down to the real-time actions needed by preventive and reacting control.	IBM
NESSI	*http://www.nessi-europe.com/Nessi/*	HP
OMEGA	*Home Gigabit Access* Gigabit home access networks (HANs) are a pivotal technology to be developed if the EU Vision of the Future Internet is to be realised. Consumers will require such HANs to be simple to install, without any new wires, and easy enough to use so that information services running on the HAN will be "just another utility," as, for instance, electricity, water and gas are today. A successful OMEGA project will demonstrate the successful realisation of a gigabit HAN. Technikon is the leading party for the development of the OMEGA Security Architecture.	IFX, TEC
PrimeLife	In their daily interaction over the Internet, individuals leave a life-long trail of personal data. Technological advances facilitate extensive data collection, unlimited storage and reuse of the individual's digital interactions. Today, individuals cannot protect their autonomy and cannot retain control over personal information, irrespective of their activities, as present information technologies hardly consider these requirements. This raises substantial new privacy challenges that are addressed by PrimeLife: how to protect privacy in emerging Internet applications such as collaborative scenarios and virtual communities; and how to maintain life-long privacy.	IBM, KUL, TUD
Reservoir	Discussion on re-use of OpenTC security components	IBM
RE-TRUST	Remote Entrusting by Run-time Software Authentication To investigate both all-in-software and hardware assisted novel methodologies in order to solve the problem of dynamic software authentication in real-time during execution by employing a trusted logic component on an untrusted machine that in turn authenticates its operation	KUL, POLITO

	continuously during run-time.	
SECRICOM	SECRICOM is proposed as a collaborative research project aiming at development of a reference security platform for EU crisis management operations with two essential ambitions: **(A)** Solve or mitigate problems of contemporary crisis communication infrastructures (Tetra, GSM, Citizen Band, IP) such as poor interoperability of specialized communication means, vulnerability against tapping and misuse, lack of possibilities to recover from failures, inability to use alternative data carrier and high deployment and operational costs. **(B)** Add new smart functions to existing services which will make the communication more effective and helpful for users. The project started in September 2008.	IAIK, IFX
SHIELDS	SHIELDS is an FP7 project concerned with model-based detection and elimination of software vulnerabilities. In this project, we conduct research and development on models for software vulnerabilities and security countermeasures, develop a repository where such models can be stored, and extend and adapt security and development tools to make use of this repository.	BME
TAS3	Trusted Architecture for Securely Shared Service http://www.tas3.eu/	KUL
TECOM	*Trusted embedded computing* R&D from a family of HW/embedded SW silicon components enforcing secure and trusted computing for the areas of consumer, computer, telecommunications, and wireless. Development of a trust concept and architecture elements usable in other European industrial segments such as automotive, industrial, aeronautics (especially in their content acquisition and payment, ticketing, and DRM aspects). Relevant European contributions related to Trusted Computing standards while keeping interoperability with existing US-led or Asian initiatives.	TEC, IFX, CEA, TUD

IST FP6		
BRIDGE	*Building Radio frequency IDentification solutions for the Global Environment*	IAIK
C@R	Collaboration Rural	IAIK
DESEREC	*"Dependability and Security by Enhanced Reconfigurability"* DESEREC will respond efficiently to the three families of incidents which can occur on a critical system: Attacks from the outside, intrinsic failures, and misbehaviour or malicious internal use.	POL (scientific leader), BME
ECRYPT	*Network of Excellence in Cryptology* http://www.ecrypt.eu.org To ensure a durable integration of European research in	KUL, RHUL, IBM, RUB

IST FP6		
	both, academia and industry, and to maintain and strengthen the European excellence in these areas.	
FIDIS	*The Future of Identity in the Information Society* http://www.fidis.net To shape the requirements for the future management of identity in the European information society and contributing to the technologies and infrastructures needed.	KUL, IBM, TUD, HP
GGCC	New C Compiler	CEA
GST	*Global System for Telematics* http://www.gstforum.org/ To create an open environment in which innovative telematics services can be developed and delivered cost-effectively.	KUL, TUM
HIDENETS	*"Highly Dependable ip-based NETworks and Services"* The aim of HIDENETS is to develop and analyze end-to-end resilience solutions for distributed applications and mobility-aware services in ubiquitous communication scenarios. Technical solutions will be developed for applications with critical dependability requirements in the context of selected use-cases of ad-hoc car-to-car communication with infrastructure service support.	BME
POSITIF	*Policy-based Security Tools and Framework* POSITIF will develop a framework and tools for policy-based protection of networked systems and applications. A multi-level policy language will be used to describe the desired security policy (high-level requirements and/or detailed controls) while a system language will be used to describe the target system (interconnection topology, functional and security capabilities).	POL
PRIME	*Privacy and Identity Management for Europe* To research and develop approaches and solutions for privacy-enhancing identity management that can make the European citizens empowered to exercise their privacy rights, and thus enable them to gain trust and confidence in the information society	HP, KUL, TUD, IBM
ReSIST NOE	ReSIST is a Network of Excellence that integrates leading researchers active in the multidisciplinary domains of Dependability, Security, and Human Factors, in order that Europe will have a well-focused coherent set of research activities aimed at ensuring that future "ubiquitous computing systems" (the immense systems of ever-evolving networks of computers and mobile devices which are needed to support and provide Ambient Intelligence), have the necessary resilience and survivability, despite any residual development and physical faults, interaction mistakes, or malicious attacks and disruptions.	IBM
RE-TRUST	*Remote Entrusting by Run-time Software Authentication* To investigate both, all-in-software and hardware-assisted	KUL, POLITO

IST FP6		
	novel methodologies, in order to solve the problem of dynamic software authentication in real-time during execution by employing a trusted logic component on an untrusted machine that in turn authenticates its operation continuously during run-time. http://re-trust.dit.unitn.it/	
ROBIN	*Open Robust Infrastructure* The objective of this Preparatory Action is to explore key technologies for a small, robust platform that can host legacy operating systems and their applications, but that is small enough to undergo formal analysis and construction techniques.	TUD
SMEPP	*Secure Middleware for Embedded Peer2Peer Platforms*	IAIK
SPEED	*Signal Processing in the Encrypted Domain* To foster the advancement of the marriage between signal processing and cryptographic techniques, both at theoretical and practical level. http://www.speedproject.eu	KUL, RUB
TEAHA	*The European Application Home Alliance* http://www.teaha.org/ To provide the suitable communication components and interoperability specification for home appliances and platforms such that products from different manufacturers will be able to interoperate in order to improve their marketability.	KUL

Table 6: Participation in EC projects

5.2 Participation in national projects

Austria		
AcTvSM	*Advanced Cryptographic Trusted Virtual Security Module* The overall goal of this project is to research a way to construct an enhanced and formally verified cryptographic security module in software using cheap off-the-shelf Trusted Computing enabled personal computers, while providing a security level close to current standalone expensive hardware security module solutions. The project started in April 2009.	IAIK
GRANDESCA	*Generating Random Numbers in the presence of SCA*	IAIK
ISCA	*Investigations on SCA*	IAIK
KIRAS	Introduction of Trusted Computing for the Austrian Government. The common goal is to foster and extend Austria's leading position in Europe in the eGoverment sector by building early awareness and migration strategies into the direction of trusted computing. Key-applications are	TEC, IAIK

	analysed throughout and potential risks are mitigated.	
QCC	*Quantum Crypto on the Chip*	IAIK
SNAP	*Secure NFC Applications*	IAIK
TOPAS	*Trust Oriented Platform for Advanced Security (FIT-IT)*	IAIK
Belgium		
BCRYPT	*Belgian Fundamental Research on Cryptography and Information Security* BCRYPT intends to perform fundamental research into a number of selected disciplines that intend to address the information security challenges we are facing. One work package focuses on mobile terminals, DRM and Trusted Computing. https://www.cosic.esat.kuleuven.be/bcrypt/	KUL, IAIK
QoE	*End-to-end Quality of Experience* This IBBT project aims at optimising user quality expectations in heterogeneous environments with a secure usage context, where resources (i.e. bandwidth and battery power) are limited and dynamic in nature, with fluctuating reliability. One work package focuses on terminal and pervasive security.	KUL
Bulgaria		
DAESPro	ICT e-Health -oriented project funded by National Science Fund	TUS
France		
CAT/U3CAT	RNTL project dedicated to static analysis techniques and tools for the C programming language. U3CAT is the follow up project.	CEA
System@Tic project PFC (Plate-Forme de Confiance)	The competitiveness pole System@Tic deals with complex hardware and software systems and is financed by the Paris area. PFC proposes to develop a platform that allows companies, administrations and citizens to build reliable and trusted information systems and associated processes. More generally, the aim is to increase the control of all the technological, legal and societal aspects bound to the development of e-activities.	CEA, RUB
Germany		
BMBF	*Easy-C* Enablers for Ambient Services and Systems	COM2
EMSCB	*European Multi-lateral Secure Computing Base* This is a German national project, started in October 2004 and sponsored by the German Ministry of Economics. The project targets the acquisition of a first Trusted Computing experience through the development of some Trusted Components, including Tamper devices, HDD encryption, DRM viewers. Relation with TSC will be established through Infineon, Ruhr University Bochum and EMSCB partners	RUB, TUD, IFX

United Kingdom		
Trust Establishment in Mobile Distributed Computing Platforms	The goal of this EPSRC-funded 3-year project (2006-2009) is to establish a secure association between a mobile wireless device (or network) and the grid. It involves studying the problem of the applicability of TC-elements to distributed systems, and grid in particular. The use of DRM techniques to protect data on the grid are being investigated.	RHUL
Trust Economics	http://www.hpl.hp.com/personal/David_Pym/NSPFullP0007E.doc	HP
XenSE	*Xen: Security Enhanced* EPSRC national research project involving CUCL, Intel Research Cambridge and CESG. This will build a prototype system for Trusted Computing which aims to be architecturally compatible with the output of the OpenTC project work. Particular focus on usability and desktop aspects.	CUCL
Italy		
MEADOW	"MEsh ADaptive hOme Wireless nets" Definition of an innovative wireless architecture to provide secure and robust integrated services for home automation and SOHO environments.	POL
OPEN-GATE	Advanced systems and services for info-mobility (vehicle-to-vehicle and vehicle-to-infrastructure).	POL

Table 7: Participation in national projects

6 Abbreviations

The abbreviations referring to the OpenTC project partners are explained below.

AMD	Advanced Micro Devices
BME	Budapest University of Technology and Economics
CEA	Commissariat à l'Energie Atomique-LIST
COM2	Comneon GmbH
CUCL	University of Cambridge Computer Laboratory
HP	Hewlett-Packard Ltd
IAIK	Graz University of Technology
IBM	IBM Research GmbH
IFX	Infineon Technologies AG
INTEK	Intek
ISE	Institute for Security and Open Methodologies
ITAS	Forschungszentrum Karlsruhe GmbH
KUL	Katholieke Universiteit Leuven
LDV	Lehrstuhl für Datenverarbeitung, Technische Universität München
POL	Politecnico di Torino
PORT	Portakal Teknoloji Egitim Danismanlik Yazilim Turizm Taahhut
RHUL	Royal Holloway and Bedford New College
RUB	Horst Goertz Institute for IT Security, Ruhr-University Bochum
SUSE	SUSE Linux Products GmbH
TEC	Technikon Forschungs- und Planungsgesellschaft mbH
TUB	TUBITAK, National Research Institute of Electronics & Cryptology
TUD	Technische Universität Dresden
TUS	Technical University of Sofia