WP5:
Dissemination

Trento - 17 October 2008
WP5 Tasks

- 5.4 Dissemination Final Report (M36)
- 5.5 Final workshop and plenary (M36)
Activities

- Conferences and workshops
- Publications
- Presentations
Workshops

- Four workshops during the second year
- with three primary objectives:
  - Stimulate discussion – brain-storming with external experts
  - Problem definition
  - Project work/tasks planning
Workshops

- Plenary Workshop - September 25-26, 2007
  September 2007 Workshop - Trento - Italy

- Fifth Quarterly Meeting - December 18-19, 2007
  December 2007 Workshop - Leuven - Belgium

- Sixth Quarterly Meeting - March 11, 2008
  March 2008 Workshop - Villach - Austria – as part of Trust 2008 event with several other EC funded projects

- Seventh Quarterly Meeting - June 19-20, 2008
  June 2008 Workshop - St. Petersburg - Russia
| Workshop:   | Plenary Workshop  
|            | 4th Quarterly Meeting |
| Date:      | 25-26 September 2007 |
| Location:  | Trento - Italy     |
| Site:      | Villa Madruzzo - Trento - Italy |
Plenary Meeting - Program

- **Presentations**
  - Bertrand Anackert  Diversity for Software Protection
  - Jan Cappaert  Self-encryption Code to Protect against Analysis and Tampering
  - Claudio Orlandi  Introduction to Secure Multiparty Computation techniques
  - Jean-Daniel Aussel  Security of Smartcards
  - Mariano Ceccato  Distributing Trust Verification
  - Haya Shulman/Amir Herzberg  White-box Remote Procedure Call
  - Moti Yung  Conference Call on Interlocking
  - Paul von Oorchoot  Conference Call on Architecture, Undebuggability
  - Christian Collberg  Conference Call on Implementation issues
  - Amir Herzberg  Conference Call  Discussion of WBRPC
  - Yoram Ofek  Introduction
  - Bart van Rijnsoever  White box cryptography and secure storage
  - Brecht Wyseur  Remote Attestation on legacy operating systems with trusted platform modules
  - Dennis Hofheinz  Obfuscation from a cryptographic perspective

- **Brief review of the work package presentations**

- **Tasks and deliverables for 2nd year**
  - WP1 - Yoram Ofek
  - WP2 - Stefano Di Carlo
  - WP3 - Brecht Wyseur
  - WP4 - Bruno Crispo

- **Structured discussion on open research challenges**
<table>
<thead>
<tr>
<th><strong>Workshop:</strong></th>
<th><strong>Fifth Quarterly Meeting</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date:</strong></td>
<td><strong>18-19 December 2007</strong></td>
</tr>
<tr>
<td><strong>Location:</strong></td>
<td><strong>Leuven - Belgium</strong></td>
</tr>
<tr>
<td><strong>Site:</strong></td>
<td><strong>Novotel Conference Hotel - Leuven - Belgium</strong></td>
</tr>
</tbody>
</table>
5th Quarterly Workshop

- Presentations
  - Sebastian Faust: Physically Observable Cryptography
  - Ahmadreza Sadeghi: Property Based Attestation
  - Dennis Hofheinzl: Publickey encryption with noninteractive opening
  - Brecht Wyseur: Computing in the Encrypted Domain
  - Mariano Ceccato: Empirical Evaluation of Protection Offered by Obfuscation
  - Thomas Herlea: RETRUST Trust Model
  - Chair: Jasvir Nagras: Open Discussion about the RETRUST Trust Model
  - Haya Shulman and Amir Herzberg: WhiteBox Remote Program Execution
  - Chair: Amir Herzberg: Open Discussion about WhiteBox Cryptography and Mobile Code
  - Stefano Di Carlo: Remote Entrusting by Remote Invariants Monitoring
  - Paolo Falcarin: Improvements Using Mobility for Remote Entrusting
  - Chair: Mariano Ceccato: Open Discussion about Generic Applications
  - Vasily Desnitsky: Entrusting Protocol Design: problem settlement, requirements and related protocols
  - Amitabh Saxena: Analysis Model
  - Christian Collberg: Analysis Model

- Discussion led by Yoram and the active participants of all WP leaders
- Discussion on Tasks
- Discussion on Deliverables
- Discussion on Milestones
6th Quarterly Workshop - Program

Workshop: Sixth Quarterly Meeting

Date: 11 March 2008

Location: Villach - Austria

Site: Congress Center Villach (CCV)
6th Quarterly Workshop - Program

- **Presentations**
  - **Invited speakers**
    - Clark Thomborson (University of Auckland) Could Software Watermarks Express Both Rules and Assurances?
    - Ahmad Sadeghi (Ruhr-University Bochum) Property-Based Attestation and Virtual TPM
    - Wulf Harder (Syncrosoft) White-box cryptography and obfuscation
  - **Re-Trust speakers**
    - Vasily Desnitsky (SPIIRAS) Development and initial analysis of entrusting protocol
    - Stefano Di Carlo (POLITO) Remote Control Flow Checking for Remote Entrusting of Software Applications
    - Pierre Girard (GEM) Javacard obfuscation
    - Anirban Majumdar (UNITN) Slicing computations
    - Jerome d’Annoville (GEM) VoIP client & demo environment
    - Stefano Di Carlo (POLITO) Candidate application / prototype

- Open discussion about project's final prototype
- Second year project's deliverables organization
7th Quarterly Workshop - Program

Workshop: Seventh Quarterly Meeting

Date: 19-20 June 2008

Location: St. Petersburg - Russia

Site: Novotel Hotel
7th Quarterly Workshop - Program

- Prof. Valery Korzhik (Invited Talk) State University of Telecommunications, Russia
  Identification and Key Distribution Based on Biometric Information

- Prof. Nikolay Moldovyan (Invited Talk) Specialized Center of Program Systems "SPECTR", Russia
  Cryptographic mechanisms for information authentication and unauthorized copying software protection

- Mariano Ceccato, Mila Dalla Preda, Anirban Majumdar, Paolo Tonella ITC-Irst, UNITN
  Remote Entrusting Remote Entrusting by OrthogonalClient Replacement

- Sebastian Faust Katholieke Universiteit Leuven
  Private Circuits Revisited: Provable Security Guarantees on Boolean Circuits

- Mariano Ceccato, Jasvir Nagra, Massimiliano Di Penta, Marco Torchiano, Paolo Tonella, Paolo Falcarin, Filippo Ricca ITC-Irst, UNITN, POLITO
  Preliminary Analysis of the Reverse Engineering Complexity

- Vasily Desnitsky, Igor Kotenko SPIIRAS
  Design and Analysis of Entrusting Protocol

- Sergey Reznik, Igor Kotenko SPIIRAS
  Analysis of Verification Tools for Security Protocols

- Sergey Reznik SPIIRAS
  Verification of Entrusting Protocol using AVISPA and Isabelle

- Alessandro Zorat UNITN
  Open discussion on Second Year Review reports

- Deliverable D2.3 Methods to dynamically replace the secure software module and to securely interlock applications with secure SW module.

- Deliverable D2.4 Protection methods for hardening the secure software module

- Deliverable D3.2 First Analysis Encrypted Code and HW assisted SW Protection

- Deliverable D4.2 Trust analysis of SW-based method

- Deliverable D4.3 Analysis of the Reverse Engineering Complexity

- Stefano Di Carlo POLITO
  Open discussion on prototype
## Publications

<table>
<thead>
<tr>
<th>Invited Talk</th>
<th>Brecht Wyseur, “Introduction to White-Box Cryptography”. At Special Summer School hosted by the ECRYPT Network of Excellence, May 16th, 2008, Crete, Greece</th>
</tr>
</thead>
</table>
## Publications

<table>
<thead>
<tr>
<th>Paper</th>
<th>Publication Details</th>
</tr>
</thead>
</table>
# Publications

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>Dries Schellekens, and Brecht Wyseur, and Bart Preneel, &quot;Remote Attestation on Legacy Operating Systems with Trusted Platform Modules&quot; in REM 2007 workshop</td>
</tr>
<tr>
<td>Paper</td>
<td>&quot;Application-oriented trust in distributed computing&quot; Riccardo Scandariato (KUL), Yoram Ofek (Trento), Paolo Falcarin, Mario Baldi (Politecnico Torino).</td>
</tr>
<tr>
<td>Paper</td>
<td>Seventh IEEE International Working Conference on Source Code Analysis and Manipulation, Paris, France, 30th September-1st October 2007, Presented by Mariano Ceccato (attended also by co-authors Jasvir Nagra, Mila dalla Preda and Paolo Tonella)</td>
</tr>
</tbody>
</table>
# Publications

<table>
<thead>
<tr>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scientific Meeting</td>
<td>Presentation by Yoram Ofek “Remote-Entrusting Paradigm for Protecting and Entrusting the Internet Infrastructure and Applications”, Israel-Italy Scientific Meeting, Tel-Aviv, Israel – May 2008</td>
</tr>
<tr>
<td>Workshop Presentation</td>
<td>Yoram Ofek; 2008 EuroTRUSTAmI 2nd edition; “Remote-Entrusting Paradigm for Protecting and Entrusting the Internet Infrastructure and Applications”</td>
</tr>
</tbody>
</table>
## Summary of Presentations

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invited talks</td>
<td>4</td>
</tr>
<tr>
<td>Papers</td>
<td>12</td>
</tr>
<tr>
<td>Scientific Meetings</td>
<td>1</td>
</tr>
<tr>
<td>Reports</td>
<td>2</td>
</tr>
<tr>
<td>Workshop Presentations</td>
<td>3</td>
</tr>
</tbody>
</table>