Sixth Framework Programme
Information Society Technology

RE-TRUST

Remote EnTrusting by RUn-time Software auTthentication

Thursday June 19th, 2008

9:50 - 9:55	Welcome and overview
9:55 - 10:45	Identification and Key Distribution Based on Biometric Information Prof. Valery Korzhik - *Invited Speaker* (State University of Telecommunications, Russia)
10:45 - 11:05	Coffee break
11:05 - 11:55	Cryptographic mechanisms for information authentication and unauthorized copying software protection Prof. Nikolay Moldovyan - *Invited Speaker* (Specialized Center of Program Systems "SPECTR", Russia)
11:55 - 12.35	Remote Entrusting by Orthogonal Client Replacement Mariano Ceccato, Mila Dalla Preda, Anirban Majumdar, Paolo Tonella (UNITN)
12:45 - 14:15	Lunch break

Sixth Framework Programme
Information Society Technology

RE-TRUST

Remote EnTrusting by RUn-time Software auTthentication

Thursday June 19th, 2008

14:15 - 14:55	Private Circuits Revisited: Provable Security Guarantees on Boolean Circuits Sebastian Faust (KUL)
14:55 - 15:35	Preliminary Analysis of the Reverse Engineering Complexity Mariano Ceccato, Jasvir Nagra, Massimiliano Di Penta, Marco Torchiano, Paolo Tonella, Paolo Falcarin, Filippo Ricca (UNITN, POLITO)
15:40 - 16:00	Coffee Break
16:00 - 16:40	Design and Analysis of Entrusting Protocol Vasily Desnitsky, Igor Kotenko (SPIIRAS)
16:40 – 17:20	Analysis of Verification Tools for Security Protocols Sergey Reznik, Igor Kotenko (SPIIRAS)
17:20 - 18:00	Verification of Entrusting Protocol using AVISPA and Isabelle Sergey Reznik (SPIIRAS)
19:00	Dinner

Sixth Framework Programme
Information Society Technology

RE-TRUST

Remote EnTrusting by RUn-time Software auTthentication

Friday June 20th, 2008

10:00 - 12:45 Open discussion on Second Year Review reports
Alessandro Zorat
(UNITN)

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*

12:45 - 14:15 Lunch break

14:15 - 15:45 Open discussion on prototype
Stefano Di Carlo
(POLITO)

15:45 - 16:00 Closing Meeting, Farewell