



First International Workshop on Remote Entrusting
October 15-16, 2008
Villa Madruzzo - Trento - Italy
Wednesday, October 15, 2008

09:00 - 10:00

Keynote Presentation

Trends and New Opportunities in Software Protection
Mikhail ATALLAH (Purdue University - USA)

10:00 - 10:30

Coffee Break

10:30 - 12:30

Session 1

Chair: Amir HERZBERG (Bar Ilan University - Israel)

Remote-Entrusting and Secure Multiparty Computation
Amitabh SAXENA (IU - Germany)

State-of-the-art in white-box cryptography

Wil MICHIELS (Philips Research - The Netherlands), Paul GORISSEN (Philips Research - The Netherlands)

Robust Combiners for White-Box Security

Amir HERZBERG (Bar Ilan University - Israel), Haya SHULMAN (Bar Ilan University - Israel)

Provably-Secure Programs Execution in Hostile Environment

Amir HERZBERG (Bar Ilan University - Israel), Haya SHULMAN (Bar Ilan University - Israel)

12:30 - 14:00

Lunch

14:00 - 15:30

Session 2

Chair: Paolo TONELLA (FBK - Italy)

An Overview of CFG Flattening

Jan CAPPAERT (KU Leuven - Belgium)

Empirical Studies

Paolo FALCARIN (Politecnico di Torino - Italy), Mariano CECCATO (FBK - Italy), Paolo TONELLA (FBK - Italy)

Software Protection and Dynamic Analysis Attacks

Anirban MAJUMDAR (University of Trento - Italy), Mariano CECCATO (FBK - Italy), Paolo TONELLA (FBK - Italy)

15:30 - 16:00

Coffee Break

16:00 - 18:00

Session 3

Chair: Mario BALDI (Politecnico di Torino - Italy)

Result Certification Against Massive Attacks in Distributed Computations

Sebastien VARRETTE (University of Luxembourg - Luxembourg), Jean-Louis ROCH (Laboratoire d'Informatique de Grenoble - LIG - France), Axel KRINGS (University of Idaho - USA)

SecNet-IE: A Secure Network for CNI Information Exchange

Fotios BASAGIANNIS (Joint Research Centre - Italy)

Secure Software Execution with the protected computing paradigm

Antonio MAÑA (Universidad de Málaga - Spain), Antonio MUÑOZ (Universidad de Málaga - Spain)

Demonstration: Using a Safe Softphone Embedded on a Dongle

Jerome D'ANNOVILLE (Gemalto - France), Jean-Daniel AUSSEL (Gemalto - France)

Thursday, October 16, 2008

09:00 - 10:30

Session 4

Chair: Igor KOTENKO (SPIIRAS - Russia)

Methods of Attack and Defense

Christian Collberg (University of Arizona - USA)

Portable Trusted File Encryption Service

Chun Hui SUEN (Lehrstuhl für Datenverarbeitung - Germany), Maximilian LOY (TUM - Germany), Toby KNOTHE (TUM - Germany)

Remote Entrusting by Orthogonal Client Replacement

Mariano CECCATO (FBK - Italy), Mila DALLA PREDÀ (University of Verona - Italy), Anirban MAJUMDAR (University of Trento - Italy), Paolo TONELLA (FBK - Italy)

10:30 - 11:00

Coffee Break

11:00 - 13:00

Session 5

Chair: Jean-Daniel AUSSEL (GEMALTO - France)

Remote Entrusting of Mobile Multi-Agent Systems

Kevin JONES (De Montfort University - UK)

Secure program partitioning for hardware-based software protection

Serge CHAUMETTE (LaBRI - Université de Bordeaux 1 - France)

A remote reconfiguration mechanism for WiseNET wireless sensor networks

Damien PIGUET (CSEM - Switzerland), Philippe DALLEMAGNE (CSEM - Switzerland), Jean-Dominique DECOTIGNIE (CSEM - Switzerland)

Attack and Tamper Detection in Remote Entrusting

Yoram OFEK (University of Trento - Italy), Anirban MAJUMDAR (University of Trento - Italy), Christian COLLBERG (University of Arizona - USA), Alessandro ZORAT (University of Trento - Italy)

13:00 - 14:00

Lunch

14:00 - 16:00

Session 6 - Panel Discussion on "What Do/Shall We Trust in Networking and Computing?"

Chair: Yoram OFEK (University of Trento - Italy)

Panel members:

Mikhail ATALLAH (Purdue University - USA)

Christian COLLBERG (University of Arizona - USA)

Antonio MAÑA (Universidad de Málaga - Spain)

Ahmad-Reza SADEGHI (Ruhr-University Bochum - Germany)

Paolo TONELLA (FBK, Trento - Italy)