SIXTH FRAMEWORK PROGRAMME - PRIORITY 2
INFORMATION SOCIETY TECHNOLOGIES (IST)

RE-TRUST:
Remote EnTrusting by RUn-time Software auThentication

"Workshop - Centro Congressi Panorama

Tuesday 19/12/2006 – Panorama

Morning Session 9.00-12.00 including Coffee Break

1. **Louis Goubin** (GEMALTO): "**Secure computations using smart cards**"

We will present some aspects of secure computations using smart cards. The problem of executing code inside the smart cards, with a focus on physical attacks will be dealt with. We will also give some ideas about the way of securely executing a code with is contained in an off-chip (insecure) memory.

2. **Mila Dalla Preda: "Code obfuscation and malware detection by abstract interpretation"**

Code obfuscation is considered as a promising defense technique against attacks to the intellectual property of software, as well as a malicious transformation commonly used by malware writers to prevent detection. In both scenarios a better understanding of the formal aspects of code obfuscation may be useful. For this reason we have investigated code obfuscation from a semantic point of view. We have proposed a characterization of code obfuscation in terms of program semantics and abstract interpretation which allows us to formally compare obfuscating and de-obfuscating techniques. The proposed semantic view has shown its potential also in the malware detection field.

3. **Igor Kotenko** (SPIIRAS): **"State of the Art in Modeling of Computer Attacks"**

It is a tutorial presentation. The talk analyses state of the art in modeling of computer attacks. We survey different attack taxonomies, attack languages and the research immediately coupled with attack modeling.

4. **Antonio Durante** (POLITO): **"Gerenic Applications"**

The talk aims at addressing the problem of identifying applications that can benefit from the RE-TRUST approach. In particular the identification of selection criteria for applications is addressed.

5. **Davide D'Aprile** (POLITO): "**Providing a RE-TRUST SDK: a (Semi) Formal Approach"**

The talk aims at presenting and collecting alternatives for SW solutions to the remote entrusting problem. Moreover, it suggests the use of formal and semi-formal methods to specify and analyze design alternatives.

SKI BREAK on MONTE BONDONE 12:00 – 16:00

Afternoon Session 16.00-19.30 including Coffee Break

1. **Ceccato Mariano** (UNITN): **"Pioneer: Verifying Code Integrity and Enforcing Untampered Code Execution on Legacy Systems"**

A primitive is proposed, called Pioneer, as a first step towards verifiable code execution on untrusted legacy hosts. Pioneer does not require any hardware support such as secure co-processors or CPU architecture extensions. Pioneer has been implemented on an Intel Pentium IV Xeon processor. Pioneer can be used as a basic building block to build security systems. It has been demonstrated by building a kernel rootkit detector.

2. **Paolo Falcarin** (POLITO): **"Design alternatives"**

I will give a presentation on design alternatives for re-trust, describing our current prototypes. My goal is trying to analyze which attacks of the table you provided, can be mitigated and which other attacks may come up using the different alternatives.

3. **Paolo Tonella** (UNITN-IRST): **"Trust and attack model"**

The remote entrusting scheme takes advantage of the network connectivity to perform authenticity verifications. Based on the assumptions on the applications that fit the remote entrusting scheme, a reference trust model is presented and discussed. Possible variants of the reference model are also presented, aimed at increasing the attack resistance. The attack model is based on assumptions on potential attackers. Four main
classes of attacks are identified and described in detail, focusing on the vulnerabilities that make each attack feasible. Sources of trust from the trust model associated with the remote entrusting scheme are related to the attacks against which they provide a typically partial defense.

4. **Vasily Desnitsky, Igor Kotenko** (SPIIRAS): **"Trust Model Supplements and Taxonomy"**

In the talk we analyze possible supplements of the Trust model of the ReTrust project architecture and suggest the taxonomy of main notions used in this model. A question about distribution of verification functions between a client program and a trusted server is raised. Some preliminary ideas on producing monitor sequences by modifying its characteristic properties for each particular verification method are proposed. We suggest a set of actions realized by the client program or the server, that can prevent any further tampered program execution and any its analysis. For more clearness we propose to use a program life cycle scheme which shows general activities of the program and the server.

5. **Vasily Desnitsky, Igor Kotenko** (SPIIRAS): **"Attack Model: Graph based Attack Representation and Taxonomy"**

In the talk we supplement an attack model of the ReTrust project architecture, suggest the taxonomy of main notions used in this model and present its possible representation based on oriented graphs. The general elements of this representation are program actions and program states. Such model heightens the
clearness of attack representation, shows action correlations in time and help to evaluate attack time complexity.

DINNER 20.00 at AGRITUR– SARDAGNA

Wednesday 20/12/2006 – Panorama

Morning Session 9.00-12.00 including Coffee Break

9:00 - 9:30 **Generic applications**

Purpose of this presentation is to described the criteria of choice for the Re-Trust target applications. Analysis of various application with those criteria.

9:30 - 10:15 **Trust model ingredients**

Presentation of relevant technologies for the project: TPM, smartcard, dongle

10:15 - 10:45 **Smartcard & PC applications**

Description of the traditional use of the smartcard on a PC.

10:45 - 11:00 **Design alternative**

Few slides on possible architecture to initiate the open session

11:00 - 12:00 **Open session on the architecture.**

Because the Session 4 is mostly target on software this is the right time to discuss on the software/hardware balance in the architecture + pros & cons on the various approaches. Active participation of partners required here

SKI BREAK on MONTE BONDONE 12:00 – 16:00

Afternoon Session 16.00-19.30 including Coffee Break

16:00 - 16:30: **Brecht Wyseur** (K.U.LEUVEN): "**White Box Cryptography**"
16:30 - 17:00: Discussion about Trust model introduction and discussion led by Jerome
17:00 – 17:30 **Thomas Herlea** (K.U.LEUVEN): **"Attack model"**

17:30 – 19:00 Open discussion on all issues – identification of publishable R&D topics:

WP2 - Step 2: Generic applications
WP2 - Step 1: Design alternatives
WP2 - Step 3: Trust model of the design alternatives with selected generic apps
WP2 - Step 4: Attack model on the design alternatives with selected generic apps
WP3 - Step 2: Generic applications
WP3 - Step 1: Design alternatives
WP3 - Step 3: Trust model of the design alternatives with selected generic apps
WP3 - Step 4: Attack model on the design alternatives with selected generic apps

Name	Short name	Country
University of Trento	UNITN	Italy
Politecnico di Torino	POLITO	Italy
Gemplus	GEM	France
Katholieke Universiteit Leuven	KUL	Belgium
St:Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences	SPIIRAS	Russia