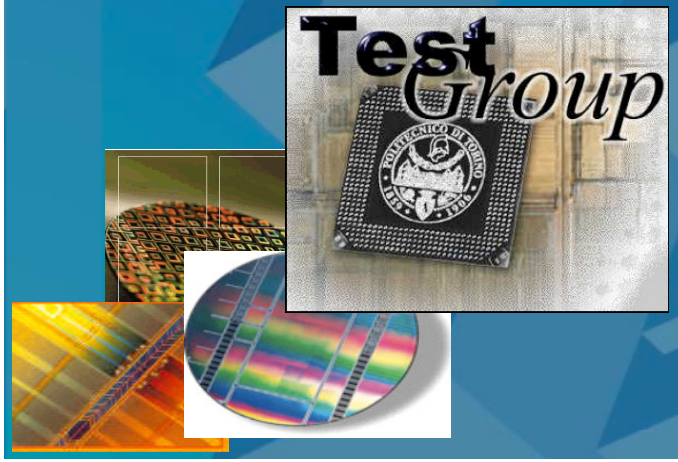
WP2 Overview

S. Di Carlo,

TESTGROUP - Politecnico di Torino (Italy)

www.testgroup.polito.it



WP2 Purpose

- To investigates software-only methodologies to implement the remote entrusting principle with the following general objectives:
  - To design and compare various SW-based alternatives;
  - To investigate and apply solutions developed for software dependability to remote entrusting;
  - To design and analyze software tamper resistance using two basic methods:
    - Dynamically replacing;
    - Increasing the complexity of software reverse engineering.

Teams

SPIIRAS

- Igor Kotenko
- Vasily Desnitsky

POLITO

(WP leader)

- Mario Baldi
- Stefano Di Carlo
- Antonio Durante
- Paolo Falcarin
- Vivek Sharma

UNITN

- Mariano Ceccato
- Mila Dalla Preda
- Jasvir Nagra
- Yoram Ofek
- Paolo Tonella

KUL

- Brecht Wyseur
- Jan Cappaert

Tasks

Task 2.5: Design of entrusting protocol (Dates: M3-24)

Task 2.4: Increased reverse engineering complexity for software protection (Dates: M3-24)

Task 2.3: Dynamic replacement for increased tamper resistance (Dates: M3-24)

Task 2.2: Secure interlocking and authenticity checking (Dates: M3-24)

Task 2.1: Trust Model (M0-M6)

Activities (1/4)

POLITO

(WP leader)

- Mario Maldi
- Stefano Di Carlo
- Paolo Falcarin
- Antonio Durante
- Vivek Sharam

POLITO1: WP2 Step 1 - Design Alternatives

Design Alternatives draft available on BSCW

Activities (1/4)

POLITO

(WP leader)

- Mario Maldi
- Stefano Di Carlo
- Paolo Falcarin
- Antonio Durante
- Vivek Sharam

POLITO1: WP2 Step 1 - Design Alternatives

POLITO2: WP2 Step 2 - Generic Applications

Generic Applications draft available on BSCW

Activities (1/4)

POLITO

(WP leader)

- Mario Maldi
- Stefano Di Carlo
- Paolo Falcarin
- Antonio Durante
- Vivek Sharam

POLITO1: WP2 Step 1 - Design Alternatives

POLITO2: WP2 Step 2 - Generic Applications

POLITO3: Hard integration between monitored application and monitor

POLITO 3.1: Remote macro flow monitoring

POLITO 3.1: Mutant software

Emerging Idea

Activities (1/4)

POLITO

(WP leader)

- Mario Maldi
- Stefano Di Carlo
- Paolo Falcarin
- Antonio Durante
- Vivek Sharam

POLITO1: WP2 Step 1 - Design Alternatives

POLITO2: WP2 Step 2 - Generic Applications

POLITO3: Hard integration between monitored application and monitor

POLITO 3.1: Remote macro flow monitoring

POLITO 3.1: Mutant software

POLITO4: Testing platform - from the chat client to VoIP

Activities (1/4)

POLITO

(WP leader)

- Mario Maldi
- Stefano Di Carlo
- Paolo Falcarin
- Antonio Durante
- Vivek Sharam

POLITO1: WP2 Step1 - Design Alternatives

POLITO2: WP2 Step 2 - Generic Applications

POLITO3: Hard integration between monitored application and monitor

POLITO3.1: Remote macro flow monitoring

POLITO3.1: Mutant software

POLITO4: Testing platform - from the chat client to VoIP

POLITO5: evaluation of OS weakness

Activities (2/4)

UNITN

- Mariano Ceccato
- Milla Dalla Preda
- Jasvir Nagra
- Yoram Ofek
- Paolo Tonella

UNITN1: WP2 - Step 3: Trust Model

Trust Model draft available on BSCW

Activities (2/4)

UNITN

- Mariano Ceccato
- Milla Dalla Preda
- Jasvir Nagra
- Yoram Ofek
- Paolo Tonella

UNITN1: WP2 - Step 3: Trust Model

UNITN2: WP2 - Step 4: Attack Model

Attack Model draft available on BSCW

Activities (2/4)

UNITN

- Mariano Ceccato
- Milla Dalla Preda
- Jasvir Nagra
- Yoram Ofek
- Paolo Tonella

UNITN1: WP2 - Step 3: Trust Model

UNITN2: WP2 - Step 4: Attack Model

UNITN3: Remote entrusting based on assertions

Emerging Idea

Activities (2/4)

UNITN

- Mariano Ceccato
- Milla Dalla Preda
- Jasvir Nagra
- Yoram Ofek
- Paolo Tonella

UNITN1: WP2 - Step 3: Trust Model

UNITN2: WP2 - Step 4: Attack Model

UNITN3: Remote entrusting based on assertions

UNITN4: Monitor factoring

Emerging Idea

Activities (2/4)

UNITN

- Mariano Ceccato
- Milla Dalla Preda
- Jasvir Nagra
- Yoram Ofek
- Paolo Tonella

UNITN1: WP2 - Step 3: Trust Model

UNITN2: WP2 - Step 4: Attack Model

UNITN3: Remote entrusting based on assertions

UNITN4: Monitor factoring

UNITN5: Software watermarking

Emerging Idea

Activities (3/4)

SPIIRAS1: Review of Trust & Attack Model

Document available?

SPIIRAS

- Igor Kotenko
- Vasily Desnitsky

Activities (3/4)

SPIIRAS1: Review of Trust & Attack Model

SPIIRAS2: Mobile module replacement issues

Document available?

SPIIRAS

- Igor Kotenko
- Vasily Desnitsky

Activities (3/4)

SPIIRAS1: Review of Trust & Attack Model

SPIIRAS2: Mobile module replacement issues

SPIIRAS

- Igor Kotenko
- Vasily Desnitsky

SPIIRAS3: Entrusting protocol design and network protocol analysis

Future activity

Activities (4/4)

KUL1: Research in Crypto-Guards

Published paper

KUL

- Brecht Wyseur
- Jan Cappaert

Activities (4/4)

KUL1: Research in Crypto-Guards

KUL

- Brecht Wyseur
- Jan Cappaert

KUL2: White-box cryptography

Paper to be published

Activities vs. Tasks