FutureTPM H2020 PROJECT: General Presentation

Coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH

coordination@futuretpm.com

Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module

The FutureTPM project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 779391.

General Project Information

- Project reference: 779391
- Project start: **1st January 2018**
- Duration: **3 years**
- Total costs/EC contribution: **EUR** € 4,868,890
- **15 partners** from **9 different European countries**
- Website: www.futuretpm.eu

Mission

- Designing and developing a **Quantum-Resistant (QR) Trusted Platform Module (TPM)**
- Provide a **new generation of TPM-based solutions,** including hardware, software and virtualization environments
- **Long-term security, privacy and operational assurance** for future ICT systems and services
- Improve the security of **Hardware Security Modules**, **Trusted Execution Environments**, **Smart Cards**, and the **Internet of Things**

Project Goal #1

- **Secure Quantum-Resistant Cryptographic Algorithms for the TPM**
  - Identify, design and develop QR algorithms for each cryptographic primitive supported by the current version of TPM
  - Development of bespoke provable-secure quantum-resistant algorithms for
    - Symmetric Cryptography
    - Asymmetric Cryptography
    - Privacy-protecting primitives, such as Direct Anonymous Attestation

Project Goal #2

- **Validation & Verification using Formal Security Analysis**
  - Provable security modelling and analysis
  - Define and design appropriate **formal methods**, including computer-aided proof systems and automated proof tools, to support the security analysis model needed to reason about the entire TPM and its functionalities

Project Goal #3

- **Implementation of Hardware, Software, and Virtual TPM**
  - Demonstrate the applicability of the identified QR algorithms to the full range of possible TPM environments
  - Implementation and rigorous evaluation of the designed QR algorithms suite in:
    - **hardware TPM (hTPM)**
    - **software TPM (sTPM)**
    - **virtual TPM (vTPM)**

Project Goal #4

- **Standardization within TCG, ISO/IEC and ETSI**
  - Development of standardisation proposals that push the state of the art in the areas of cryptography and the TPM itself
  - Involve the technical committees of the relevant standards bodies, notably **ISO, IEC, ETSI** and the **TCG**

Project Goal #5

- **Provision of Run-Time Risk Assessment and Vulnerability Analysis Methodologies**
  - FutureTPM will design **risk analysis methods** that target all the phases of a system’s development lifecycle, from design time to near real-time risk quantification of newly identified attacks

FutureTPM Use Cases

Online Banking

- To isolate the e-payment process in a more protected context so as to provide enhanced security levels against unintentional data leakage and malicious apps

Activity Tracking

- To increase the trust of users of cloud-based activity tracking services in the security and privacy properties of their stored and leveraged data

Device Management

- To help protect private keys stored on routers, mobile devices, and IoT devices against compromise or misuse by malicious applications

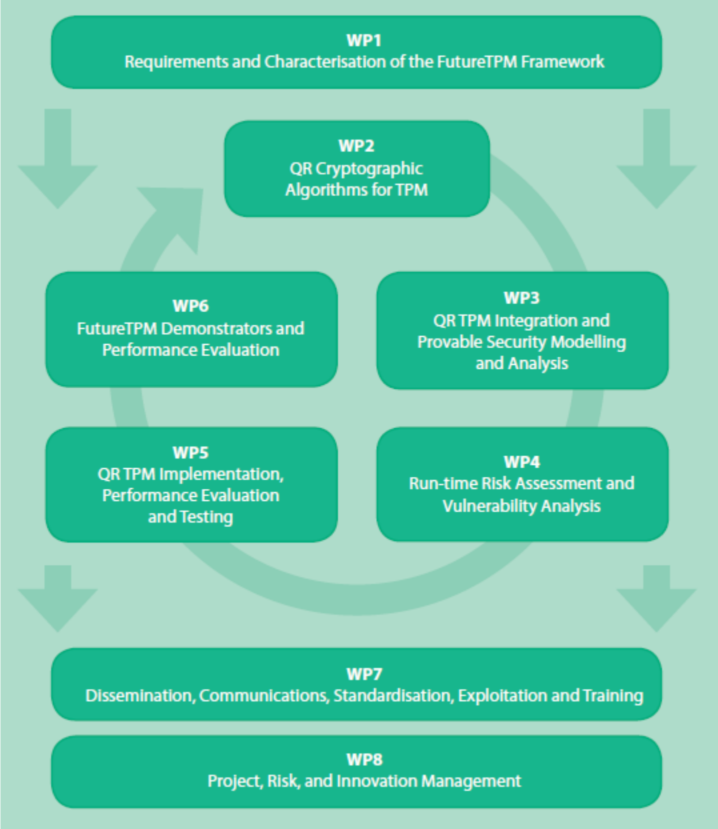
Impact

- FutureTPM will provide a **new generation of TPM-based solutions**
- FutureTPM will fill the gaps that currently threaten the long-term security properties of trusted computing
- Will enable FutureTPM systems to **generate a secure root of trust** that can be used
  - for interacting with Cloud services,
  - accessing corporate services,
  - performing banking and eCommerce transactions,
  - along with a wide range of other services.

Impact

- Adoption guidelines of such hardware-solutions can benefit not only the industries of interest but also other domains such as **Intelligent Transportation Systems**, **eHealth**, **Industry 4.0**, **Digital Media and Content Protection**, etc.

WPs Interaction



WP1
Requirements and Characterisation of the FutureTPM Framework

WP2
QR Cryptographic Algorithms for TPM

WP6
FutureTPM Demonstrators and Performance Evaluation

WP3
QR TPM Integration and Provable Security Modelling and Analysis

WP5
QR TPM Implementation, Performance Evaluation and Testing

WP4
Run-time Risk Assessment and Vulnerability Analysis

WP7
Dissemination, Communications, Standardisation, Exploitation and Training

WP8
Project, Risk, and Innovation Management

Contacts

Project Coordinator

MMag. Martina Truskaller
TECHNIKON Forschungs- und
Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach, Austria
Tel.: +43 4242 233 55
Email: cooridnation@futuretpm.com

Website: www.futuretpm.eu

- FutureTPM_H2020 FOLLOW US ON twitter
- FutureTPM-Project LinkedIn

Technical Leader

Prof. Liqun CHEN
University of Surrey
388 Stag Hill
Guildford GU2 7XH
United Kingdom
Email: liqun.chen@surrey.ac.uk

and Dr. Thanassis GIANNETSOS
Technical University of Denmark
Anker Engelunds Vej 1 Bygning 101A,
2800 Kgs. Lyngby, Denmark
Email: atgi@dtu.dk

Project Partners

TECHNIKON

Surrey Centre for Cyber Security SCCS

Technical University of Denmark DTU

UBITECH ubiquitous solutions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

IBM Research

UNIVERSITY OF BIRMINGHAM

infineon

uni.lu | SnT securityandtrust.lu

Suite5 We Deliver Intelligence

inesc id lisboa

UNIVERSITY OF PIRAEUS

HUAWEI

INDEV

FutureTPM Grant Agreement No. 779391

“The FutureTPM project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 779391.”

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55   Fax: +43 4242 233 55 77
E-Mail: coordination@futuretpm.eu

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.