Securing a quantum-computer world: Optimizing the Connected World - FutureTPM, a European H2020 research project, is set to develop quantum-resistant security components

The European cooperative research project FutureTPM officially started on January the 1st 2018 and is coordinated by the Austrian company TECHNIKON. Under the technical lead of the University of Surrey, the project team will research a Quantum-Resistant (QR) Trusted Platform Module (TPM) by designing and developing QR algorithms suitable for inclusion in a TPM. Such a security anchor, also known as root-of-trust, is commonly used in domains with high appetence for security and trust, such as finance and banking (secure mobile payment), wearables (activity tracking) and device management. The project runs for 36 months and receives funding from the European Union under grant agreement number 779391.

With the emergence of the Internet of Things (IoT) industry's digital transformation has begun, bringing with it new challenges, and adding an urgency to old unsolved challenges. Security, in particular, is one of the main concerns, due in part, to recent developments in quantum computing. Experts believe, that once a fault- tolerant universal quantum computer is available, which may still take many years from now, it will be capable of solving complex mathematical problems, including current public-key cryptographic solutions, which could be compromised. Nevertheless, TPMs shouldn't be appropriately secure and robust only for today, but should be designed for long-term use. As a result, the necessity for quantum-resistant (QR) cryptographic algorithms gets higher.

To tackle these challenges, **FutureTPM** will provide a new generation of TPM-based solutions, including hardware, software and virtualization environments, incorporating robust and physically secured QR cryptographic primitives. This will allow long-term security, privacy and operational assurance in the complex domain of future ICT systems and services. Moreover, **FutureTPM** will focus on the following **technical objectives**:

- Design and development of a holistic TPM-based framework
- Threat security analysis for TPM cryptographic functionality
- Identification and implementation of a reactive, run-time risk assessment model
- Validation of applicability, usability, effectiveness and value of FutureTPM concept
- Effective engagement with industry
- Wide communication and scientific dissemination of FutureTPM

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

The goal is to enable a smooth transition from current TPM environments, based on traditional cryptography, to systems providing enhanced security through QR cryptographic functions, including secured authentication, encryption and signing functions, thus, turning the host device into a "hardened" security token that may also remain secure long-term against an enhanced threat landscape in quantum computing deployments.

Use cases in online banking, activity tracking and device management will provide environments and applications to validate the **FutureTPM** framework.

The **FutureTPM** consortium consists of 14 highly qualified industrial and academic partners from various backgrounds and 9 different countries (Austria, United Kingdom, Cyprus, Switzerland, Germany, Luxembourg, Ireland, Portugal and Greece), making it well-positioned to achieve its objectives.

The FutureTPM partners are:

- TECHNIKON Forschungs- und Planungsgesellschaft mbH , Austria
- University of Surrey, United Kingdom
- UBITECH Limited, Cyprus
- Royal Holloway and Bedford New College, United Kingdom
- IBM Research GmbH, Switzerland
- The University of Birmingham, United Kingdom
- Infineon Technologies AG, Germany
- Infineon Technologies Austria AG, Austria
- Université du Luxembourg, Luxembourg
- Suite5 Data Intelligence Solutions Limited, Ireland
- INESC-ID – Instituto de Engenhariade Sistemas e Computadores, Investigacao e Desenvolvimento em Lisboa, Portugal
- University of Piraeus Research Center, Greece
- Huawei Technologies Düsseldorf GmbH, Germany
- VIVA Payment Services SA, Greece

The official Kick-Off meeting will take place from 23rd-24th January 2018 and will be hosted by Infineon Technologies Austria AG in Graz. Stefan Rohringer, Infineon development center Graz: „Infineon, the leading provider of security solutions, is ready to provide a smooth transition from today's security protocols to next-generation post-quantum cryptography (PQC). To better respond to security threats that are yet to come, we continuously collaborate with the academic community, customers and partners. The EU-project FutureTPM pushes for future standards that can be executed efficiently and securely on small and embedded devices."

For more information, please visit http://www.futuretpm.eu [coming soon]

Contact Information:

Project Coordinator:
MMag. Martina TRUSKALLER
TECHNIKON Forschungs- und Planungsgesellschaft mbH

Burgplatz 3a
9500 Villach

Scientific/Technical Lead:
Prof. Liqun CHEN and
Dr. Thanassis GIANNETSOS
University of Surrey

388 Stag Hill
Guildford GU2 7XH

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

Österreich
Email: coordination@futuretpm.eu

United Kingdom
Email: liqun.chen@surrey.ac.uk
a.giannetsos@surrey.ac.uk

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