Introduction to FutureTPM
Project status and today's agenda

1st Workshop, 19th October 2018, Lisbon

Liqun Chen, Thanassis Giannetsos

liqun.chen@surrey.ac.uk
a.giannetsos@surrey.ac.uk

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
- 14 partners from 9 different European countries
- Website: www.futuretpm.eu

FutureTPM Mission

- Quantum-Resistant Trusted Platform Module (QR TPM)
- Full range of **implementation** environments
  - hardware-TPM (demonstrator)
  - software-TPM (demonstrator)
  - virtual-TPM (demonstrator)
- Formal **security analysis**
- **Run-time risk assessment** towards fine-grained trust based on the envisioned use cases

Why QR TPM?

- trusted computing
- hardware security
- QR TPM
- trusted platform module
- quantum-resistant cryptography

Current state: TPM's cryptographic algorithms

Cryptographic Co-processor
- Asymmetric encryption
- Symmetric encryption
- Signatures & DAA
- Message authentication code
- Hash functions
- Key exchange

TPM 1.2 supports
- RSA encryption
- RSA signature
- RSA-DAA
- SHA-1
- HMAC
- AES (optional)

TPM 2.0 supports
- Asymmetric encryption
  - RSA encryption and EC encryption
- Symmetric encryption
  - AES, SM4, Triple DES, …
- Signature
  - RSA signature and EC signature
- DAA
  - EC-DAA
- Message authentication code
  - HMAC
- Hash functions
  - SHA-1, SHA-256, SM3, …
- Key exchange
  - ECDH

When a large-scale quantum computer becomes a reality

Cryptographic Co-processor
- Asymmetric encryption
- Symmetric encryption
- Signatures & DAA
- Message authentication code
- Hash functions
- Key exchange

TPM 1.2 supports
- RSA encryption BROKEN
- RSA signature BROKEN
- RSA-DAA BROKEN
- SHA-1
- HMAC
- AES (optional)

TPM 2.0 supports
- Asymmetric encryption
  - RSA encryption and EC encryption BROKEN
- Symmetric encryption
  - AES, SM4, Triple DES, …
- Signature
  - RSA signature and EC signature BROKEN
- DAA
  - EC-DAA BROKEN
- Message authentication code
  - HMAC
- Hash functions
  - SHA-1, SHA-256, SM3, …
- Key exchange
  - ECDH BROKEN

Three types of TPM QR algorithms

- Symmetric algorithms
  - Hash, MAC, symmetric encryption
  - Existing algorithms will not directly be broken, but key/block lengths may need to be increased
- Conventional asymmetric algorithms
  - Encryption, signature, key exchange
  - Existing algorithms will be broken
  - Many QR algorithms have been developed (e.g., submissions to NIST PQC)
- Asymmetric privacy-preserving algorithms
  - Direct Anonymous Attestation (DAA)
  - Not in the scope of NIST
  - Not much research so far

Other post-quantum crypto projects

- **PQCRYPTO**
  - Design of high-security post-quantum PK systems
- **SAFECrypto**
  - Practical, robust and physically secure post-quantum crypto solutions
- **PROMETHEUS**
  - Quantum-resistant privacy-preserving cryptographic mechanisms

FutureTPM Mission

Mission: *Design a* ***QR TPM*** *covering the full range of* ***implementation environments*** *coupled with* ***formal security analysis*** *and* ***run-time risk assessment****, and evaluated under assumptions of realistic deployment scenarios*

- 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

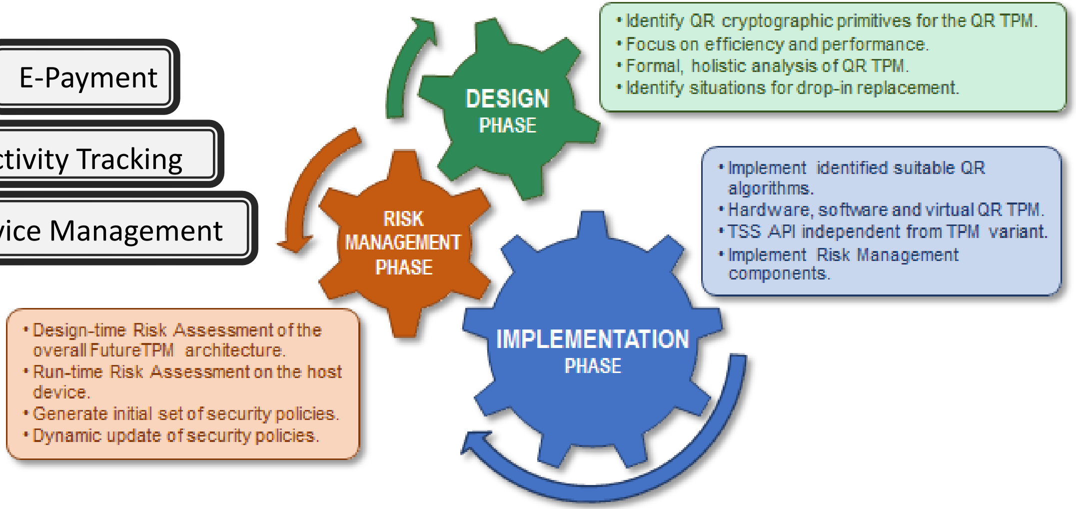
FutureTPM Mission (cont)

TPM as a major building block for enhanced security & privacy in various application domains

- Secure & Dependable Communication
- Authenticity and Integrity
- Privacy and Data protection
- Security Hardware
- Data consistency
- Security Architecture

- Performance & Efficiency
- Cost
- Security-Processes/ Management
- Security Evolution & Maintenance
- Security Metrics

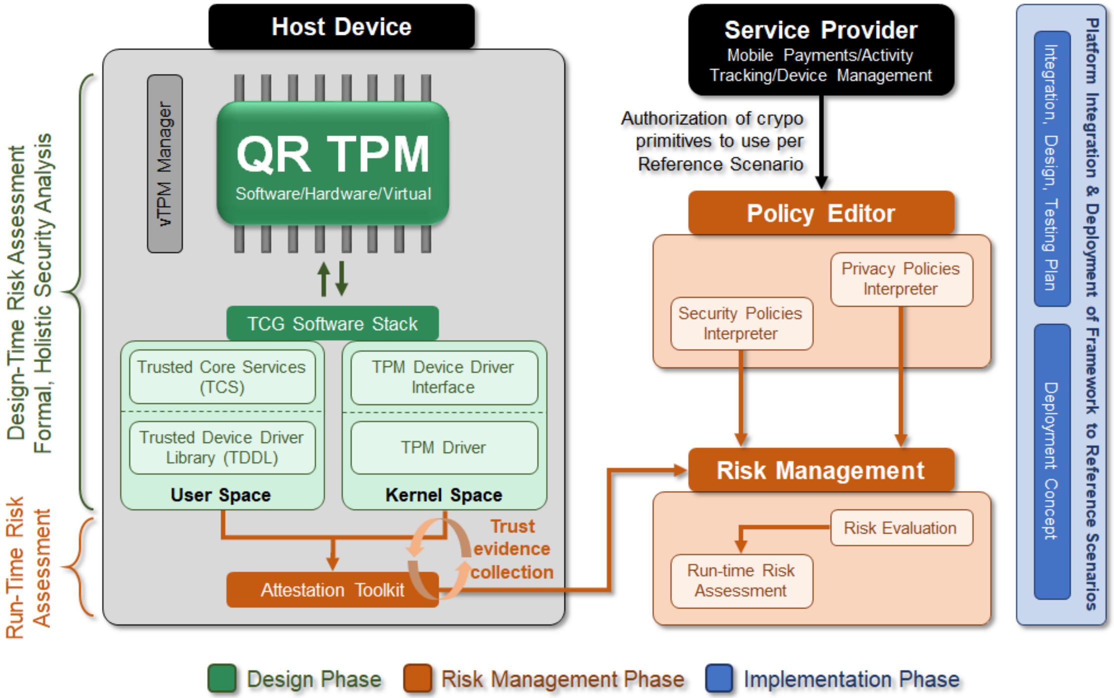
- E-Payment
- Activity Tracking
- Device Management



Reactive security mechanisms & updates

FutureTPM Conceptual Architecture

- **FutureTPM QR Design:**
  - QR Crypto Primitives
- **FutureTPM Implementation:**
  - HW, SW, VM-based
  - Secure Storage, Attestation
- **Risk Management:**
  - Risks, threats, assets, attack types, vulnerabilities, control elements
  - Fine-grains security policies
- **Security Modelling:**
  - Threats (physical/software/remote) to be considered

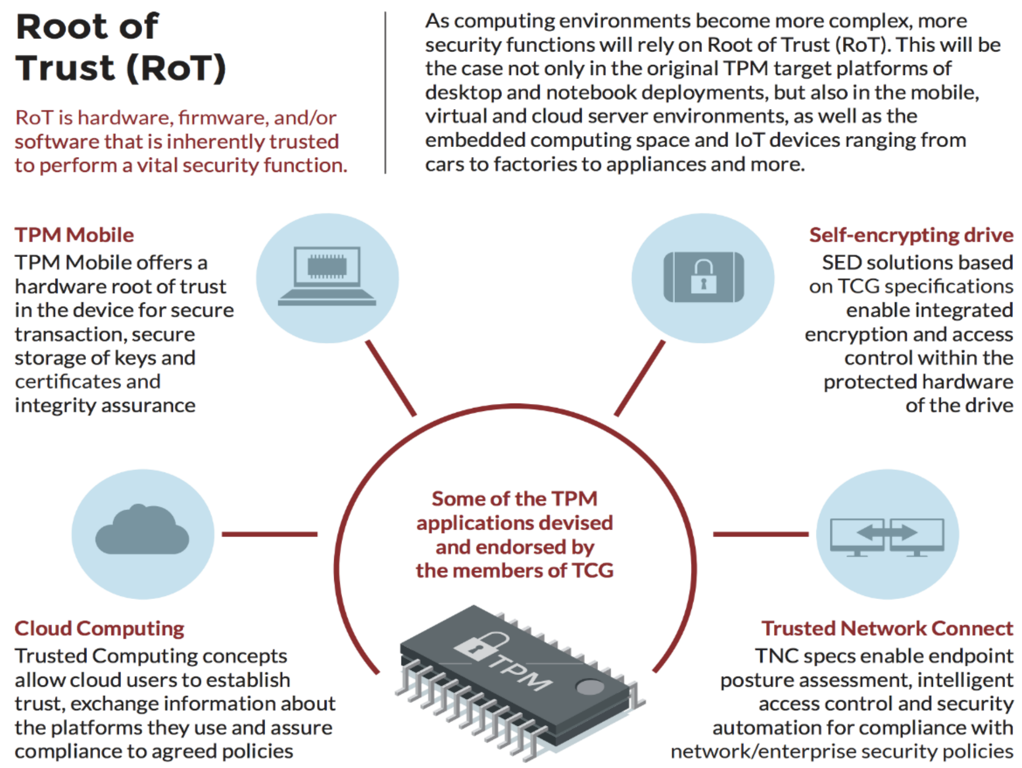


TPM Services

- **Attestation**
- **Protected Storage**
- **Platform Authentication**
- **…**

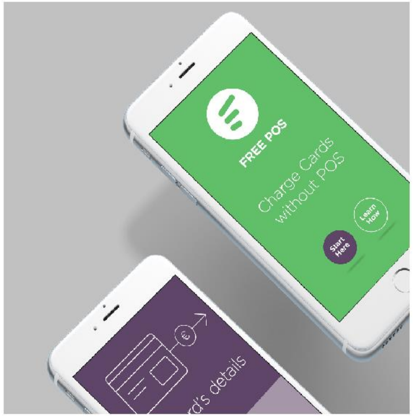
Cryptographic Primitives

- Hash functions
- Block ciphers
- Digital Signatures
- Public-key Encryption & Key Exchange
- Direct Anonymous Attestation



Secure Mobile Wallet and Payments

- Use of **FreePOS** application as a testbed developed by **INDEV, GR**
  - One of the top finance apps in Greece – tens of thousands active users
  - **Hardware-based TPM**
- **Token- based** authentication
  - *Depends on OS level security*
- OAuth 2.0 with PCI compliant services



- **Confidentiality**
  - TPC key storage persistency -> token storage
- **Integrity**
  - HMAC digital signatures for financial data integrity
- **Authentication**
- **Key Exchange**

Personal Activity and Health Kit Data Tracking

- Use of **S5 Tracker** application as a testbed developed by **SUITE5 Data Intelligence Solutions, UK**
- **Data Anonymization** and **Privacy Preservation**
  - *Generation of "User Personas"*
  - **Software-based TPM**
- **Privacy**, confidentiality and security at the edge
  - Direct Anonymous Attestation
- **Data Integrity**
  - HMAC digital signatures for financial data integrity
- **Secure Data Sharing**
  - No data leakage

Device Management

- **Secure management** of network infrastructures by HWDU
  - Integrity of identified devices
  - **Virtual-based TPM**
- **Device Identification:**
  - *TPM key generation and persistent storage*
- **Software Integrity**
  - TPM Platform Configuration Registers (PCRs)
- **Data Integrity and Confidentiality**
  - Key usage TPM policies

2 Phase Testing

- **1st Phase Testing:**
  - Internal, small-scale, lab-test
  - **M18** (MS4) - first release of SW-based TSS + QR TPM + RA framework
  - **M21** (MS5) - first release of FutureTPM framework
  - **M24** – 1st Demonstration Phase + 2nd FutureTPM Workshop
- **2nd Phase Testing:**
  - Internal, large-scale, hybrid test
  - **M27** (MS7) – Final release of FutureTPM framework (including all TPM implementations)
  - **M33** (MS8) – 2nd Demonstration Phase + 3rd FutureTPM Workshop

08:30 - 09:00	FutureTPM Workshop Registration	
Session 1 - Welcome and Introduction to FutureTPM Workshop		
09:00 - 09:20	Introduction to FutureTPM Project status and today's agenda	Liqun Chen & Thanassis Giannetsos (University of Surrey)
09:20 - 10:00	The Future of Trusted Computing	Steve Hanna (Trusted Computing Group)
10:00 - 10:40	NIST Cryptographic Standards for Trusted Platform in Quantum Era	Lily Chen (NIST - National Institue of Standards and Technology)
10:40 - 11:00	Coffee Break	
Session 2 - The use of Trusted Computing towards Enhanced Security and Privacy		
11:00 - 11:20	Comprehensive Remote Attestaion for Device Management	Roberto Sassu & Silviu Vlasceanu (Huawei)
11:20 - 11:40	Empowering Trust and Security on Sharing Personal Activity Data A FutureTPM Use Case	Thanassis Giannetsos (University of Surrey)
11:40 - 12:00	Secure Mobile Wallet and Payments	Fanis Sklinos (Indev Software SA)
12:00 - 13:00	Lunch Break	
13:00 - 13:20	A Platform Manufacturer´s View of TPMs	Carey Huscroft (HP Labs)
13:20 - 13:45	Thales and Trusted Computing	Adrian Waller (Thales UK)

Session 3 - Other EU Initiatives towards QR Crypto		
13:45 - 14:15	Results of PQCrypto (ICT-645622)	Tanja Lange (University of Eindhoven)
14:15 - 14:45	SAFEcrypto: Secure Architectures of Future Emerging Cryptography	Adrian Waller (Thales UK)
14:45 - 15:15	PROMETHEUS or how to provide Quantum-Resistant Privacy-Preserving Cryptographic Mechanisms	Sébastien Canard (Orange)
15:15 - 15:45	Using and Breaking Hardware Security Anchors	David Oswald (University of Birmingham)
15:45 - 16:00	Coffee Break	
Panel Discussion		
16:00 - 16:45	Innovating with Trusted Computing: The Journey towards the Implementation of a Quantum-Resistant TPM	**Moderator:** Liqun Chen **Panelists:** Lily Chen, Steve Hanna, Christian Hanser, Carey Huscroft, Tanja Lange, Adrian Waller
Session 4 - Quantum-Resistant TSS Implementation		
16:45 - 17:05	PQC TSS and PQC TPM - a Prototype	Andreas Fuchs (Fraunhofer SIT)
17:05 - 17:25	Implementation of the FutureTPM QR Hardware TPM Demonstrator	Christian Hanser (Infineon)
17:25 - 17:45	PQ Direct Anonymous Attestation	Paulo Martins (INESC-ID)
17:45 - 18:00	FutureTPM Workshop Closing Remarks	Liqun Chen & Thanassis Giannetsos (University of Surrey)

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