Datensicherheit im Quantenzeitalter:
Optimierung der vernetzten Welt – Welche Verbesserungen das europäische H2020 Forschungsprojekt FutureTPM bringt
Entwicklung quantenresistenter Sicherheitskomponenten (Trusted Platform Modules)

Das europäische Forschungsprojekt FutureTPM wurde am 1. Jänner 2018 unter Koordination der TECHNIKON Forschungs- und Planungsgesellschaft mbH aus Villach gestartet. Das Kick-Off-Meeting mit allen internationalen Partnern findet heute bei Infineon in Graz statt. Das Projektteam unter der technischen Leitung von Dr. Thanassis Giannetsos und Prof. Liqun Chen (University of Surrey) wird in den nächsten 36 Monaten ein quantenresistentes Trusted Platform Module (TPM) entwickeln. Dieser sogenannte Vertrauensanker (root-of-trust) wird unter anderem in Anwendungen im Finanzsektor (secure mobile payment) oder Wearables (Activity Tracking) sowie bei zentral verwalteten Business Laptops/PCs eingesetzt.

Nach sechs Jahrzehnten seit Beginn der Computer-Revolution, vier Jahrzehnten seit der Erfindung des Mikroprozessors, und zwei Jahrzehnten nach dem Aufstieg des modernen Internets, sind wir nun in der Lage, eine vernetzte Welt zu ermöglichen, wobei kein Teilbereich der digitalen Welt unberührt bleibt. Allerdings sind an diese neuen Möglichkeiten auch neue Herausforderungen geknüpft, welche insbesondere in sicherheitskritischen Domänen im Vordergrund stehen. Um diesen Herausforderungen entgegen zu wirken, hat sich das Projektteam FutureTPM als Ziel gesetzt ein quantenresistentes (QR) Trusted Platform Module unter Zuhilfenahme sogenannter Post-Quantum-Kryptographie (PQC) zu entwickeln.

Doch wozu werden QR kryptografische Algorithmen benötigt? Kryptografische Funktionen, wie sie in einem TPM verbaut sind, sollen nicht nur kurzfristig ausreichend sicher bleiben, sondern auch langfristig durch ihre Sicherheit überzeugen. Durch die Entstehung von Quanten-Computern geraten allerdings einige gefragte und bekannte kryptografische Lösungen in Bedrängnis. Aufgrund dessen wird das Bedürfnis nach den sogenannten quantenresistenten (kryptografischen) Lösungen immer größer. Darauf basierend, setzte sich auch FutureTPM als Ziel, QR-Kryptoalgorithmen, welche mit einem TPM kompatibel sind, zu identifizieren, weiterzuentwickeln und damit Robustheit auf lange Sicht zu ermöglichen. Das Design wird in drei besonderen Anwendungsfällen (Mobile Wallet Payments, Activity Tracking und Device Management) getestet und anhand formeller Sicherheitsanalysen validiert.

Das FutureTPM Projekt hat vielfältige Auswirkungen auf die Öffentlichkeit:

- Erhöhung der Vertrauenswürdigkeit der europäischen ICT-Dienste und -Produkte
- Stärkung der Wettbewerbsfähigkeit der EU-Kryptographie durch die Bereitstellung eines neuen Satzes von QR-Kryptographie-Primitiven und Algorithmen
- Implementierung der entwickelten QR-Algorithmen und Validierung in Bezug auf verbesserte Leistung und Effizienz (der Kryptographie) über den Stand der Technik hinaus

Das FutureTPM Konsortium besteht aus 14 hochkarätigen industriellen und akademischen Partnern aus 9 verschiedenen europäischen Ländern (Österreich, Großbritannien, Zypern, Schweiz, Deutschland, Luxemburg, Irland, Portugal und Griechenland), die den Projekterfolg mit ihrem Know-How und ihrer Erfahrung unterstützen werden.

Die FutureTPM Partner sind:

- TECHNIKON Forschungs- und Planungsgesellschaft mbH, Österreich
- University of Surrey, Großbritannien
- UBITECH Limited, Zypern
- Royal Holloway and Bedford New College, Großbritannien
- IBM Research GmbH, Schweiz
- The University of Birmingham, Großbritannien
- Infineon Technologies AG, Deutschland
- Infineon Technologies Austria AG, Österreich
- Université du Luxembourg, Luxemburg
- Suite5 Data Intelligence Solutions Limited, Irland
- INESC-ID – Instituto de Engenhariade Sistemas e Computadores, Investigacao e Desenvolvimento em Lisboa, Portugal
- University of Piraeus Research Center, Griechenland
- Huawei Technologies Düsseldorf GmbH, Deutschland
- VIVA Payment Services SA, Griechenland

Das offizielle Kick-Off Meeting findet von 23.-24. Jänner 2018 in Graz statt. Gastgeber ist die Infineon Technologies Austria AG. Stefan Rohringer, Leiter des Infineon Entwicklungszentrums Graz: „Als führender Anbieter von Sicherheitschips bereitet Infineon den reibungslosen Übergang von heutigen Sicherheitsprotokollen auf die Post-Quantum-Kryptographie vor. Um besser auf künftige Sicherheitsbedrohungen reagieren zu können, arbeiten wir kontinuierlich mit Wissenschaftlern, Kunden und Partnern zusammen. Das Projekt FutureTPM geht einen weiteren Schritt in der Entwicklung künftiger Standards, die auch auf kleinen und eingebetteten Systemen effizient und zuverlässig ausgeführt werden können.“ Im Rahmen des Kick-Offs werden die Mitglieder des FutureTPM Konsortiums die weitere Zusammenarbeit der Projektpartner organisieren und technische Aspekte und Details der einzelnen Projektphasen klären.

Weitere Informationen finden Sie unter http://www.futuretpm.eu [coming soon]

Kontaktinformation:

Projektkoordinator:
MMag. Martina TRUSKALLER
TECHNIKON Forschungs- und Planungsgesellschaft mbH

Burgplatz 3a
9500 Villach
Österreich
Email: coordination@futuretpm.eu

Technische Leiter:
Dr. Thanassis GIANNETSOS and
Prof. Liqun Chen
University of Surrey

388 Stag Hill
Guildford GU2 7XH
United Kingdom
Email: a.giannetsos@surrey.ac.uk

liqun.chen@surrey.ac.uk