Designing and Implementing Cryptographic Primitives for Next-Gen TPMs

Master´s Degree Graduation Project

TECHNIKON

var motivation;

Trusted Platform Modules (TPMs) are playing a vital role in modern cryptography. They ensure the system security and privacy and act as an anchor or better say as the Root-of-Trust of computing systems.
Therefore, it is crucial that the cryptographic functions, such as used in nowadays TPMs, should not only be secure today but also remain secure for a long time. The vision of our international research project, **FutureTPM (779391)**, is to provide a new generation of TPM-based solutions, incorporating robust and physically secure Quantum-Resistant (QR) cryptographic primitives.
The goal is to enable a smooth transition from current TPM environments, sustain secure authentication, encryption and signing functions and turn the host device into a "hardened" security token that may also remain secure for a long-term against attacks performed by large-scale quantum computers.

function project_description () {

% You will work on the reference architecture of the next-generation quantum-resistant TPMs.

% You will get the possibilities to perform technical and security requirement analysis in terms of the next-generation QR TPM in order to increase your experience in both, the theoretical and practical manner.

% You will be part of the development team when designing and implementing QR cryptographic primitives for the next-generation TPM.

% You will be able to accompany the path from the project idea, over specifying use-cases and application scenarios, to implementing a prototype based on hardware-entangled security features.

Your work will result in a research report or scientific paper. Coincidentally, the project fit for a graduations project (Master's degree) as well as semester abroad projects of about 5 months (1 semester). Our staff will provide technical guidance. Candidates can drive on scientific guidance provided by several leading partners in the cryptography and quantum computing domain.

In detail, the following graduation project is open for application:

Identification, design and implementation of (QR) cryptographic primitives with respect to symmetric and asymmetric cryptographic algorithms in Trusted Platform Modules.

}

function getJob () { return (‘€‘)

We consider a gross payment sum of EUR 10.000,00 for each project assuming that the candidate is eligible for receiving payments either as “Werkstudent” or “Student” under the Austrian law for employment.

}

environment.includes (

You will be working for the research department of TECHNIKON and become part of the **FutureTPM project team**. You will be granted access to our laboratory equipment and security hardware.

)

if (qualifications) {

- % Profound knowledge and experience in terms of cryptographic primitives and algorithms
- % Interest on software and hardware security and relevant upcoming topics in the crypto world
- % Understanding for software and hardware integrations as well as background on cryptographic algorithms, related mathematics or information theory of advantage
- % Well-found English proficiency, capacity for teamwork as well as personal commitment and sense of responsibility

} return contact;

Attracted your interest? Send your questions or even better your application to:
Mr. DI Mario Muenzer at **coordination@futuretpm.eu**

TECHNIKON
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
www.technikon.com