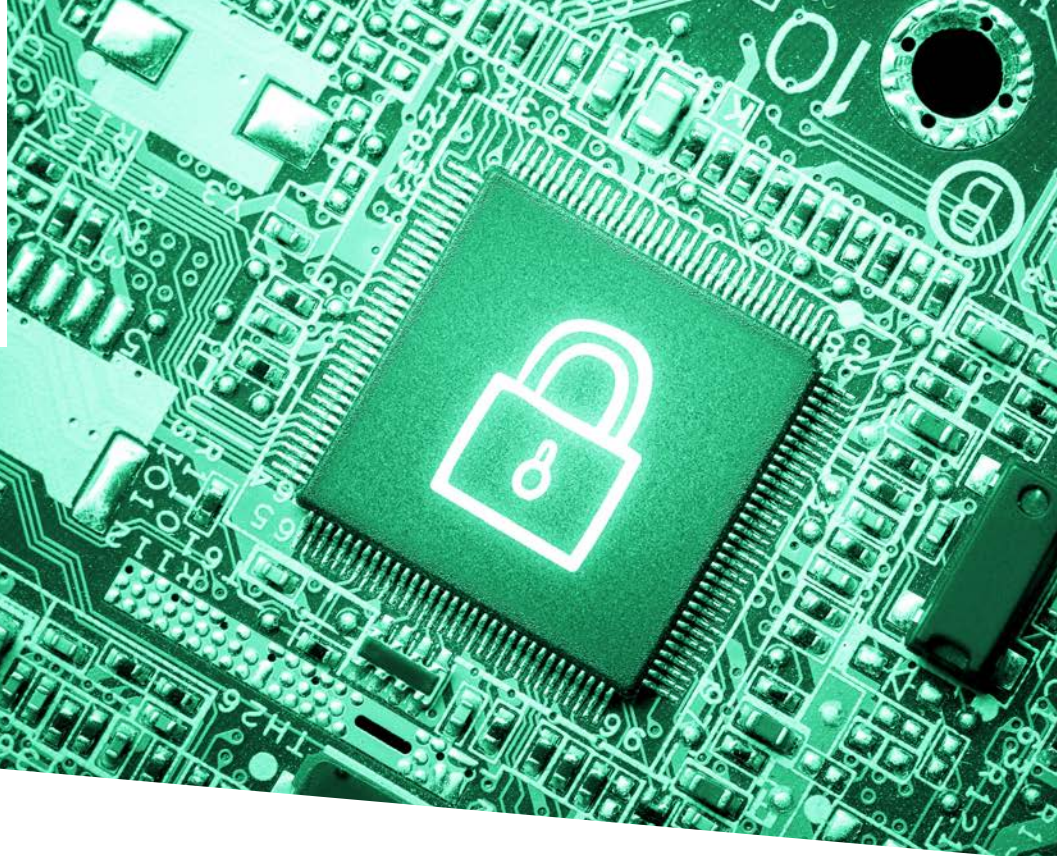


FutureTPM



Newsletter / June 2019 – Issue 4



Thanassis Giannetsos

Technical Lead, FutureTPM
Technical University of Denmark

Table of Contents

1. Project Status Update
2. 1st Workshop on Cyber-Security Arms Race (CYSARM) Technical and AB Meeting
3. A Closer Look at FutureTPM Use Cases
4. Submitted Public Deliverables
5. Dissemination: upcoming

Almost Halfway & Well on Track

Project status update from Thanassis Giannetsos

Having reached almost the halfway point of the FutureTPM project, we are delighted to announce that all core research and technical milestones have been successfully achieved and we are now entering the evaluation, validation and refinement phases with planned activities for setting up and testing the FutureTPM framework in the context of the three use cases.

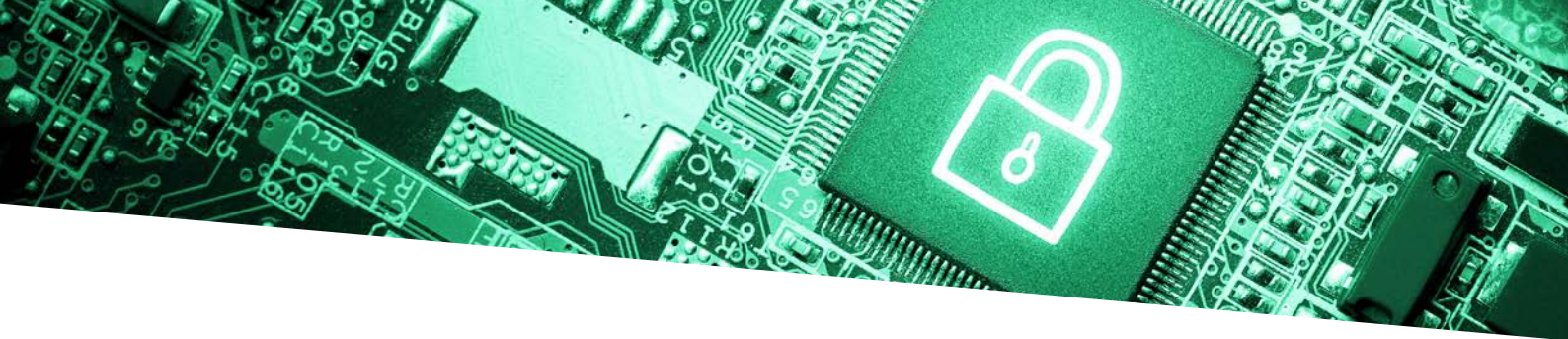
The project has been working in parallel in all core technical and implementation & demonstration work packages with tangible outcomes in all considered research avenues:

- Investigation and identification of the set of QR cryptographic primitives (i.e., symmetric, asymmetric and privacy-preserving) that were deemed as the most appropriate for implementation in the various TPM environments. Examples include some of the most prominent families of algorithms, including also a newly developed QR Direct Anonymous Attestation (DAA) protocol (to be available by end of 2019). The first

version of the software-based TPM will be available by end of June, 2019 whereas the first version of the hardware- and virtual-based TPM will be available by end of September, 2019;

- Early results on the security modelling and analysis of the TPM have also enabled the design of a complete, run-time Risk Assessment and Vulnerability Analysis framework including also a novel control-flow attestation toolkit capable of providing strong guarantees against a wide range of attack vectors. A first implementation will be available by end of September 2019;

- The consortium has started working towards the full implementation and integration of the envisioned use cases, with the current focus being on the setup of the appropriate environments for experimentation whereas the first version will be ready by end of September, 2019 for the first round of evaluation and validation (by end of December, 2019).



1ST WORKSHOP ON CYBER-SECURITY ARMS RACE (CYSARM) — CALL FOR PAPERS

1ST WORKSHOP ON CYBER-SECURITY ARMS RACE (CYSARM)

NOVEMBER 15, 2019 — LONDON, UK



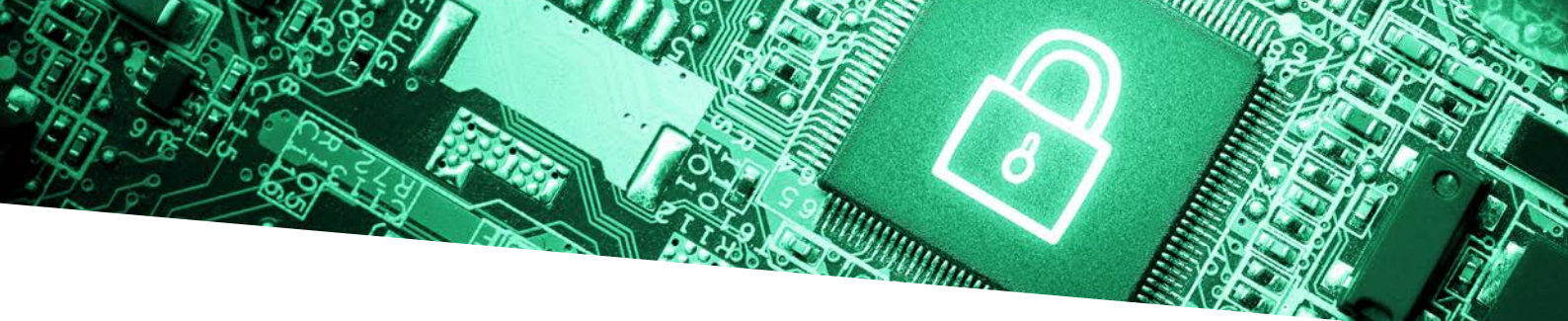
The FutureTPM project is happy to announce the upcoming first edition of the **CYSARM workshop** (1st Workshop on Cyber-Security Arms Race (www.cysarm.org)), co-located with the 26th ACM Conference on Computer and Communications Security (CCS). The workshop, which will be held in London, UK, on November 15th, 2019, is a joint initiative of the most pertinent cyber-security and crypto-related EU H2020 projects: FutureTPM, ASTRID, PROMETHEUS and PAPAAYA.

Cybersecurity is a complex ecosystem that is based on several contradicting requirements. For this reason, it is often defined as an arms race between attackers and defenders: for example, when a new security model or algorithm is devised, it could act as a double-edged sword since it might

both enhance the security posture of a system and introduce additional vulnerabilities. The goal of CYSARM workshop is to foster collaboration and discussion among cyber-security researchers and practitioners to discuss the various facets and trade-offs of cybersecurity and how new security technologies and algorithms might impact the security of existing or future security models.

Important dates:

- **Submission deadline: 14 July 2019 11:59 PM (AoE, UTC-12)**
- **Notification of acceptance: 7 August 2019**
- **Camera-ready papers: 30 August 2019 (hard deadline)**
- **Workshop date: 15 November 2019**



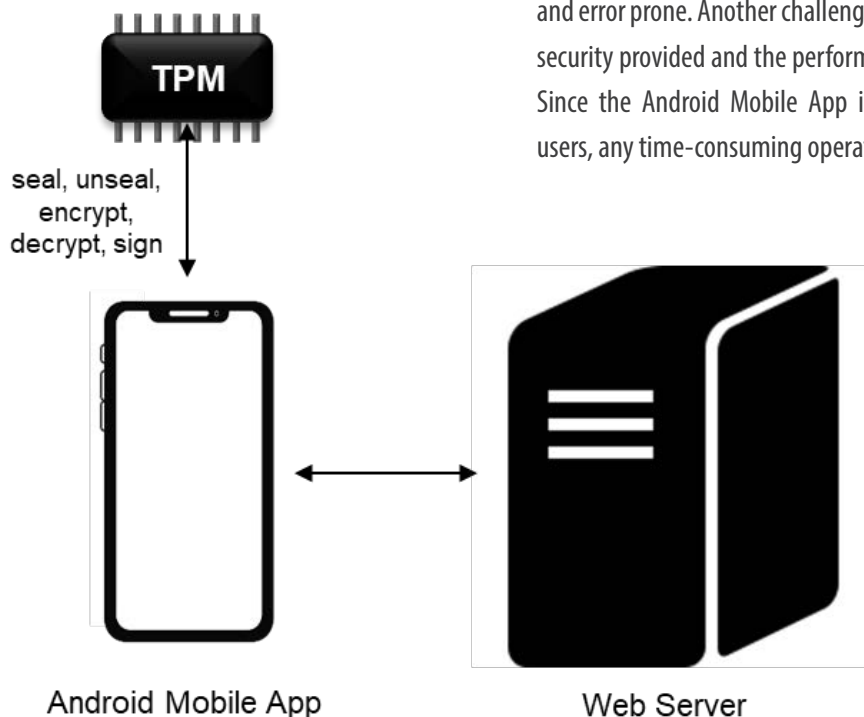
A CLOSER LOOK AT FUTURE TPM USE CASES

Use Case 1: Secure Mobile Wallet and Payments

WHAT IS THE USE CASE ABOUT?

Mobile wallets and e-payment services have become widespread as they enable an easy payment process that is complementary to traditional methods. However, using a mobile wallet over open devices and networks poses new security challenges.

Therefore, security becomes now fundamental to the overall functionality of the mobile payment transaction itself. One key security and trust issue is how the sensitive tokens are handled by the mobile payment app and the corresponding backend infrastructure. To this end, the “INDEV Secure Mobile Wallet and Payments” use case works on protecting sensitive data by making it tamper-proof, demonstrating how the use of trusted computing technologies (supporting QR crypto primitives) can benefit mobile wallet and payment applications to be secure and trusted.

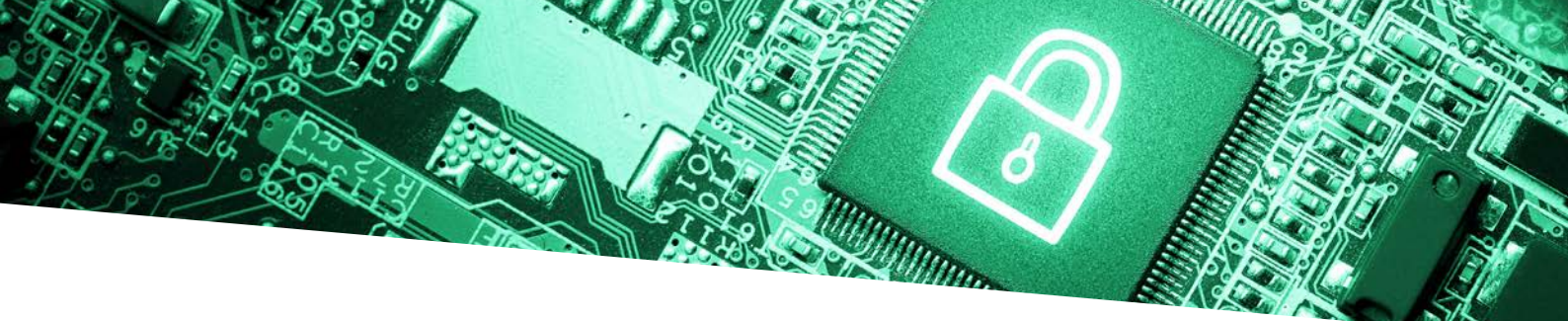


WHAT IS THE CURRENT STATUS OF IMPLEMENTATION?

Currently, the consortium is working on an Android application to use core TPM functionalities (i.e., sealing, device integrity) towards securing sensitive tokens with an authorization policy while having the necessary guarantees on the device integrity through appropriate calculations of the applications installed in the TPM-equipped mobile device. More specifically, we are examining existing solutions in Android, such as TSSDroid and Trusty TEE, to shift to the HW QR-TPM upon the release of the first version. In parallel, we have examined the hardware TPM capabilities on the server side.

WHAT ARE THE MAIN CHALLENGES?

This use case is very challenging due to many difficulties in adopting TPMs in mobile devices. More precisely, to-date, there is no official API definition available for Android TSS and most of the Java-based implementations (such as jTSS) are complex and error prone. Another challenge is the balance between the security provided and the performance of internal operations: Since the Android Mobile App is focused on high demand users, any time-consuming operation will be unaccepted.



A CLOSER LOOK AT FUTURE TPM USE CASES

Use Case 2: Activity Tracking

WHAT IS THE USE CASE ABOUT?

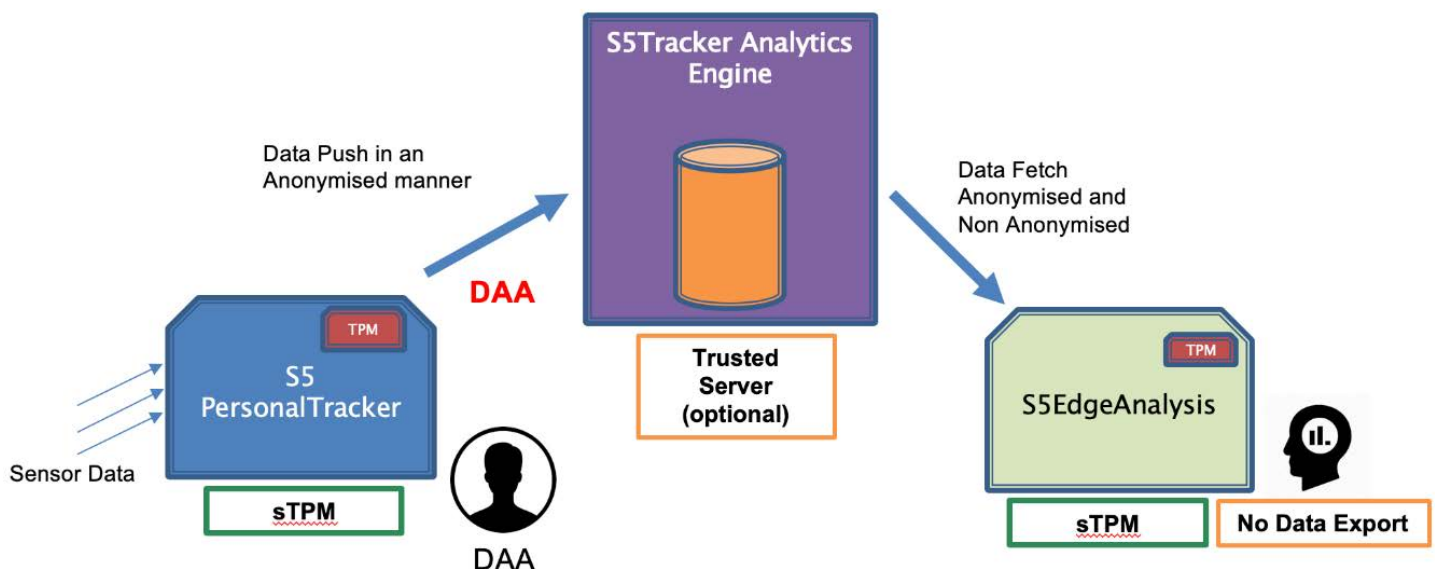
The **S5 Activity Tracker use case aims to demonstrate how FutureTPM can be used to increase security and trust for personal data sharing in the post-quantum era.** Built on the existing S5 Activity Tracker infrastructure, the use case will demonstrate how personal activity data generated at users' side (through wearables, IoT devices, etc.) can be securely and anonymously transferred and stored in a central repository that is capable of sharing analytics with trusted third party entities (such as physicians or care providers) without disclosing any personal or sensitive information from the user.

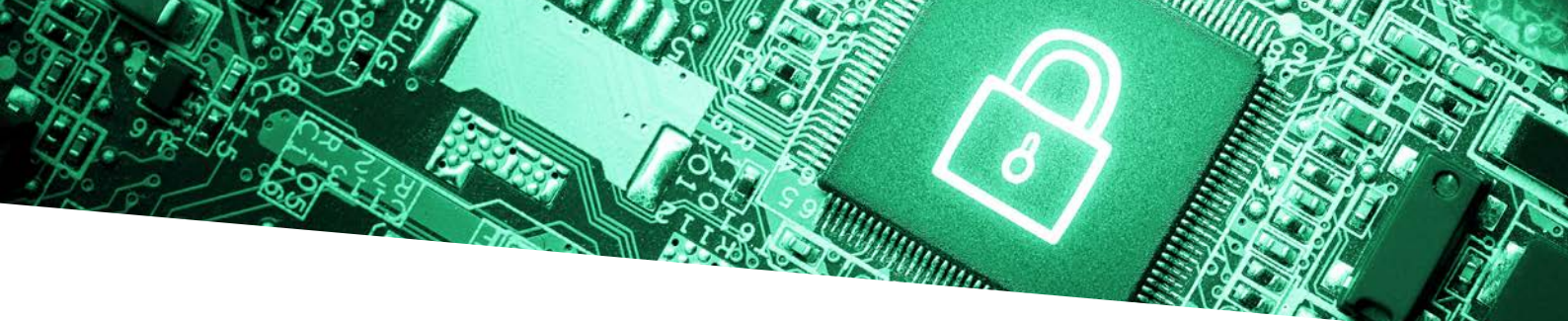
WHAT IS THE CURRENT STATUS OF IMPLEMENTATION?

Suite5 is the responsible developer of the use case. Currently the use case is aiming to explore the use of Software-based TPMs and advanced crypto primitives, mainly Direct Anonymous Attestation (DAA), for enhanced security and privacy between the end-user side (data collection points) and the centrally managed cloud-based analytics infrastructure.

WHAT ARE THE MAIN CHALLENGES?

The primary challenge of the use case has to do with the application of DAA in this data sharing scheme; specifically, with the application of DAA using PQ algorithms aiming to not impact the performance requirements of the application.





A CLOSER LOOK AT FUTURE TPM USE CASES

Use Case 3:
Device Management

WHAT IS THE USE CASE ABOUT?

The device management use case focuses on the management of network infrastructures, such as those found in enterprise organizations. Companies

often define strict security policies to protect their valuable data and rely on the network infrastructure to support them. However, this protection could be breached if a network device is compromised. In such a scenario, private, financial, or employee information could be leaked and redirected to points of exploitation or exposed for later brute-forcing.

The demonstrator will show how management of the network infrastructure can be enhanced to take into account the integrity of the network devices with techniques introduced by trusted computing.

WHAT IS THE CURRENT STATUS OF IMPLEMENTATION?

Huawei, as the leading partner of this use case, is currently focusing on the following:

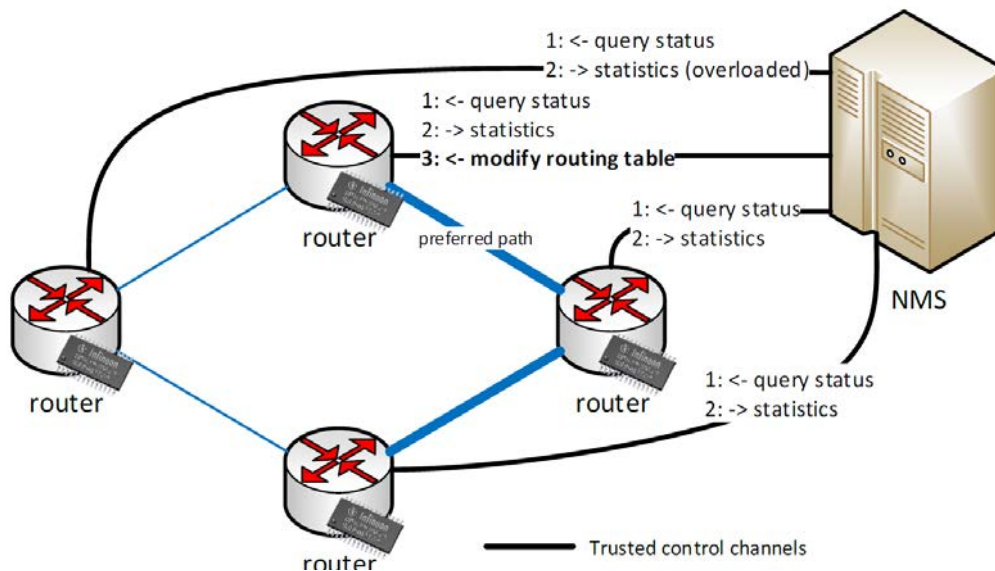
Support for predictable integrity state of the system software based on the Digest Lists extension to Linux Integrity Measurement Architecture (IMA): prototype ready

Support for integrity verification of mutable files based on Integrity Models extension to Linux IMA: prototype in progress
Simple Remote Attestation Protocol: prototype ready

WHAT ARE THE MAIN CHALLENGES?

Without trusted computing or similar technologies, routers face the following challenges:

- **Device identification:** Identification is usually done by establishing a secure channel between the Network Management System (NMS) and the device, where the device must prove the possession of a key; however, the key is not strongly bound to the device and may be leaked or duplicated to other devices;
- **Software integrity:** The NMS cannot determine if the management commands sent to the controlled devices have been processed successfully. It also does not have trustworthy evidence on the integrity of the device, exposing network traffic to routing through potentially compromised devices;
- **Integrity and confidentiality of device configuration:** Such data is often stored in plain text and integrity is not verified; also, sensitive parts of the configuration can be leaked by a potentially compromised device.



UPCOMING PUBLIC DELIVERABLES

[Public RTD Deliverables published on FutureTPM](#)

First Report on the Security of the TPM

Initial report discussing issues related to modelling and reasoning about trust, usage and authorization policies, and the TPM's cryptographic primitives, protocols, and the realization of access control.

Runtime Risk Assessment, Resilience and Mitigation Planning - First Release

Initial report on describing the complementary functionalities of the already designed Risk Assessment and Vulnerability Analysis framework. It will describe how to handle unacceptable calculated risks by inferring (using backward-chaining techniques) the optimal mitigation actions (i.e., properties that have to be reactively attested) that have to be applied.

First version of TPM implementation


First version of SW based QR TSS and QR TPM.

Technical Integration Points and Testing Plan

Having the architecture proposed for the FutureTPM framework as a base reference, this report will present the interactions among the individual core components of the system, describing their interfaces and how they will be integrated to work as a whole.

UPCOMING DISSEMINATION ACTIVITIES

NIST Second PQC Standardization Conference

August 22nd, 2019 | @ University of California, Santa Barbara, 

1st Workshop on Cyber-Security Arms Race (CYSARM)

November 15th, 2019 | @ London, UK
co-located with the 26th ACM Conference on Computer and Communications Security sponsored by H2020 FutureTPM, ASTRID, PAPAYA & PROMETHEUS projects 

(More information on page 2)

REPRESENTATIVE PUBLICATIONS

FutureTPM provides open access to all published articles, on the ZENODO platform. 

Evaluation of Password Hashing Schemes in Open Source Web Platforms



Authors: Ntantogian Christoforos; Maliaros Stefanos; Xenakis Christos

L-DAA: Lattice-Based Direct Anonymous Attestation



Authors: Nada El Kassem and Liqun Chen (Surrey), Jan Camenisch (IBM), Rachid El Bansarkhani (TU Darmstadt), Ali El Kaafarani and Patrick Hough (Oxford)

HyPoRes: An Hybrid Representation System for ECC



Authors: Paulo Martins and Leonel Sousa (INESC-ID), Jérémy Marrez and Jean-Claude Bajard (Sorbonne Université)

A Survey of Voice and Communication Protection Solutions Against Wiretapping



Authors: Ntantogian Christoforos; Veroni Eleni; Karopoulos Georgios; Xenakis Christos



SUBMITTED PUBLIC DELIVERABLES

[Public RTD Deliverables published on FutureTPM](#)

Threat Modelling & Risk Assessment Methodology

The Deliverable provides the details of the Risk Assessment (RA) methodology that will be followed in FutureTPM towards the design and implementation of a holistic RA framework capable of providing vulnerability analysis and policy enforcement during both design- and run-time. It also provides the analysis of the TPM commands that will be used as the baseline for our investigation (per reference scenario). Each reference scenario will focus on one main TPM functionality including Sealing, Direct Anonymous Attestation (DAA) and Key Creation and Storage.



Follow FutureTPM on:



futuretpm.eu



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