# Remote Attestation

by

**Huzaifa Hashim and Raja Rafey**

Senior Year Project in Computer Science

Submission: December 2, 2020 Supervisor: Prof. Jurgen Schonwalder

Jacobs University Bremen | Department of Computer Science and Electrical Engineering

## English: Declaration of Authorship

I hereby declare that the thesis submitted was created and written solely by myself without any external support. Any sources, direct or indirect, are marked as such. I am aware of the fact that the contents of the thesis in digital form may be revised with regard to usage of unauthorized aid as well as whether the whole or parts of it may be identified as plagiarism. I do agree my work to be entered into a database for it to be compared with existing sources, where it will remain in order to enable further comparisons with future theses. This does not grant any rights of reproduction and usage, however.

This document was neither presented to any other examination board nor has it been published.

## German: ErklÃ¤rung der Autorenschaft (Urheberschaft)

Ich erklÃ¤re hiermit, dass die vorliegende Arbeit ohne fremde Hilfe ausschlieÃŸlich von mir erstellt und geschrieben worden ist. Jedwede verwendeten Quellen, direkter oder indirekter Art, sind als solche kenntlich gemacht worden. Mir ist die Tatsache bewusst, dass der Inhalt der Thesis in digitaler Form geprÃ¼ft werden kann im Hinblick darauf, ob es sich ganz oder in Teilen um ein Plagiat handelt. Ich bin damit einverstanden, dass meine Arbeit in einer Datenbank eingegeben werden kann, um mit bereits bestehenden Quellen verglichen zu werden und dort auch verbleibt, um mit zukÃ¼nftigen Arbeiten verglichen werden zu kÃ¶nnen. Dies berechtigt jedoch nicht zur Verwendung oder VervielfÃ¤ltigung.

Diese Arbeit wurde noch keiner anderen PrÃ¼fungsbehÃ¶rde vorgelegt noch wurde sie bisher verÃ¶ffentlicht.

Date, Signature

# Abstract

Consider this a separate document, although it is submitted together with the rest. The abstract aims at another audience than the rest of the proposal. It is directed at the final decision maker or generalist, who typically is not an expert at all in your field, but more a manager kind of person. Thus, don't go into any technical description in the abstract, but use it to motivate the work and to highlight the importance of your project.

(target size: 15-20 lines)

# Contents

# 1 Introduction

(target size: 1-2 pages)
This section will provide a basic introduction to the technical concepts of Remote Attestation. The aim is to provide an introduction that introduces the phenomenon and explains its need in a world with more devices than humans with enormous amounts of data, and the possibility of that data to be compromised. The aim is not to ”fix everything” but to identify shortcomings, and discuss possible improvements.

## 1.1 Fundamental Remote Attestation Concepts

This part will attempt to technically connect to the main underlying concepts which are important to understand the schematics of the procedure, and the entities that are typically involved in Remote Attestation Procedures. The aim is to provide a glossary of sorts that help the reader understand what follows.

## 1.2 Current Research and Aims of this Report

This section will summarize the current research that exists which is elaborated in the following sections. The aim of this report is to prototype a YANG Module Functionality for TPM Based Challenge Response Remote Attestation and adding it together with the FraunHofer implementation, instead of using CBOR (as currently done in the codebase), to allow for better scaleability and interoperability between devices running Remote Attestation Procedures. This area requires a decent amount of research and is currently a work in progress.

# 2 Statement and Motivation of Research

(target size: 5-10 pages)
This section intends to establish the stated goals of the project (what exactly are we trying to do? What are we trying to answer? What is the relevance/significance of our research and experimental work).

To this end, we hope to implement a YANG Data Model instead of using CBOR Web Tokens for Challenge Response Based Remote Attestation Procedures in the FraunHofer IETF Proof on Concept RATS Implementation which can be found at this URL: https://github.com/Fraunhofer-SIT/charra

This section will delve into the existent technology by introducing TPM’s. The brunt of this section will be based on the knowledge gained by reading the pool of collected Academic Papers on Wireless Sensor Networks, especially the Paper ”Attestation in Wireless Sensor Networks: A Survey,” supplemented by additional already existent work in WSNs (SWATT, PIV, SCUBA, SEDA etc.)

The section starts with a brief introduction and then moves to subsections covering the following:

### 2.1 Applications of Remote Attestation

This section will introduce a higher level description of the procedure as a precursor to introducing the use cases for remote attestation which discuss the access authentication, application authentication and trusted link in Remote Attestation. This stresses the relevance of the scheme and the practical implications of it.

### 2.2 Remote Attestation and the Trusted Platform Module

This section introduces the Trusted Platform Module (TPM) by including current work and research. This is an industry standard as every device (mostly) has a manufacturer issued TPM which can be used by the Remote Attestation procedure as a means to improve the validity of the attestation scheme.

### 2.3 Limitations, Assumptions, and Attacks

This section talk about Wireless Sensor Networks and defines different instances of Remote Attestation and the assumptions and limitations of the scheme. This grounds the research questions into what can and cannot be achieved because the paper sets itself up to improve the probabilistic guarantee of the prover.

# 3 Standardization Work for Remote Attestation

(target size: 5-10 pages)

This section will provide an overview of our investigation of the latest Standardization Work for Remote Attestation Procedures conducted by the IETF.

This is the technical core of the thesis. Here you lay out your how you answered your research question, you specify your design of experiments or simulations, point out difficulties that you encountered, etc.

## 3.1 Architecture

This part will attempt to provide an architectural overview of Generic Remote Attestation Procedures, along with addressing basic Topological Models, Trust Models, The Roles and Conceptual Messages involved, as well as Claim Encoding Formats and Freshness.

## 3.2 Interaction Models

This part introduces Direct Anonymous Attestation for privacy and confidentiality preserving requirements, as well as describe Interaction Models for Remote Attestation Procedures.

## 3.3 TPM based Remote Integrity Verification

This part outlines the Remote Integrity Verification problem, and delves into concepts such as RIV Keying, Information Flow, PCR Allocations, Attestation Logs, Reference Integrity Manifests (RIMs), Data Transport and Encoding, and security elements which are essential to defining scale-able Remote Attestation Procedures working with commercial networking devices.

## 3.4 YANG Data Module for Challenge Response Based Remote Attestation

This part attempts to introduce the YANG Data Module described in the IETF Internet Draft draft-ietf-rats-yang-tpm-charra-03, which defines a YANG RPC and a minimal datastore required to retrieve attestation Evidence about Integrity Measurements.

# 4 Evaluation of the Investigation

(target size: 5-10 pages)

## 4.1 Investigating Linux APIs for accessing TPMs

This part will attempt to investigate the most relevant aspects of the TPM 2.0 Software Stack (TPM2-TSS) from its tpm2-tss open source implementation on github.

## 4.2 Investigating the FraunHofer SIT Proof of Concept Implementation for the IETF Challenge Response Based Remote Attestation Procedures Draft - CHARRA

This part will investigate the working of the FraunHofer SIT CodeBase and evaluate its scope, shortcoming, and areas of further development.

## 4.3 A YANG Data Model Prototype for CHARRA

This part will attempt to provide a YANG Data Model Functionality for the FraunHofer CodeBase to allow for better interoperability for Remote Attestation Procedures involving commercial networking products running different data parsers.

# 5 Conclusions

(target size: 1/2 pages)
Summarize the main aspects and results of the research project. Provide an answer to the research questions stated earlier.