Claims Verification for Remote Attestation on Trusted Platform Modules

by

Huzaifa Hashim

Senior Year Project in Computer Science

Submission: December 9, 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 to the phenomenon and the scope of the report. It ends with a brief summary of what follows in the next sections.

2 Statement and Motivation of Research

(target size: 5-10 pages)
This section intends to establish the stated goals of the project

To this end, this project aims to analyze the challenge-response remote attestation procedure with a focus on the verification of the data that is exchanged between the verifier, attester, and the relying party. This section will preferably include a primer for the language that will be used to describe and analyze the attestation scheme.

The reference adaptation of the challenge-response attestation scheme is the implementation by Fraunhofer that can be found at the following link: https://github.com/Fraunhofer-SIT/charra

2.1 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.

2.2 Remote Attestation and the Trusted Platform Module

This section introduces the TPM as a piece of hardware which acts as a root of trust for attestation. A large part of attestation schemes which follow a hardware based approach is directly associated with TPM's. The paper on Wireless Sensor Nodes is analyzed here with a focus on the attacks that can be carried out, identifying the key components and different existing solutions which are already put forth to prevent said attacks.

An important observation is that even when attestation schemes cover the entirety of the memory of the attester, it is still a "probabilistic guarantee of the integrity of the prover".

3 Description of the Investigation

(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.

3.1 RATS Architecture

Assessing the architecture is important because it mentions key concepts which build to the project aim of improving the reliability of the attestation and identifying the lack in the simulator program from Fraunhofer.

The architecture file ”Remote Attestation Procedures Architecture draft-ietf-rats-architecture-08” is an important part because it provides an overview of the Appraisal Policy used by the verifier and key attributes such as ”Freshness” of the data which is a security primitive. This section will provide an overview of the topology, trust models, and the role of different parties involved.

3.2 Interaction Models

This part introduces Direct Anonymous Attestation for privacy and confidentiality preserving requirements, and more importantly explain different models from the challenge-response based attestation scheme. It also builds upon the challenge-response information and provides a juxtaposition of the different models that could be used to set up attestation in different devices.

3.3 Fraunhofer’s Implementation of CHARRA and accessing a TPM

This part delves into the implementation which uses Mbed-Crypto (now moved to Mbed TLS), CBOR with t_cose, CoAP, and the TSS libraries to build a TPM simulator which can model an attestation scheme. The implementation verifies attestation signatures, but does not verify nonces and PCR’s which is functionality still left to be implemented.

4 Evaluation of the Investigation

(target size: 5-10 pages)

4.1 The TPM2 Software Stack and Linux API's

This part introduces the software that is originally developed by Microsoft to access the TPM on a device running Windows. It has a working adaptation for devices running Linux and allows access to functions within libraries set PCR values and initiate an attestation procedure between remote servers. The Fraunhofer codebase is an adaptation of the TSS to run challenge-response based attestation.

4.2 Investigating the Fraunhofer implementation and its pitfalls

Main attempt would be to look at the lacking implementations identified and analyze the need to extend the verification in the context of research and state of the art already identified previously based on readings. This focuses on different properties that are associated with the shared data such as "freshness" which makes verifying the nonces shared pivotal for the attestation integrity. This part also briefly goes over the CWT and JWT tokens which are used for exchanging claims between parties. The implementation relies on COSE defined in RFC 8152 and implements Entity Attestation Tokens https://tools.ietf.org/html/draft-ietf-rats-eat-01 which also lacks interoperability but since Raja is working on YANG, this would probably not be the focus.

Another interesting thing that could be looked into is the implementation of blockwise CoAP data transfers which requires further research but my initial understanding is that it has to do with the size of the data shared between two parties and is more effective somehow?

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.

References

[1] Rodrigo Vieira Steiner and Emil Lupu. 2016. Attestation in wireless sensor networks: A survey. ACM Comput. Surv. 49, 3, Article 51 (September 2016), 31 pages. DOI: http://dx.doi.org/10.1145/2988546

[2] P. Maene, J. Götzfried, R. de Clercq, T. Müller, F. Freiling and I. Verbauwhede, "Hardware-Based Trusted Computing Architectures for Isolation and Attestation," in IEEE Transactions on Computers, vol. 67, no. 3, pp. 361-374, 1 March 2018, doi: 10.1109/TC.2017.2647955.

[3] S. Zeitouni et al., "ATRIUM: Runtime attestation resilient under memory attacks," 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, 2017, pp. 384-391, doi: 10.1109/ICCAD.2017.8203803.

[4] Dries Schellekens, Brecht Wyseur, and Bart Preneel. 2008. Remote attestation on legacy operating systems with trusted platform modules. Sci. Comput. Program. 74, 1–2 (December, 2008), 13–22. DOI:https://doi.org/10.1016/j.scico.2008.09.005

[5] Remote Attestation Procedures Architecture, Retrieved: https://tools.ietf.org/pdf/draft-ietf-rats-architecture-08.pdf

[6] Reference Interaction Models for Remote Attestation Procedures, Retrieved: https://tools.ietf.org/pdf/draft-ietf-rats-reference-interaction-models-01.pdf