SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Establishing trust in an updatable fTPM using remote attestation

Andreas Korb

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Establishing trust in an updatable fTPM using remote attestation

Herstellung von Vertrauen in ein aktualisierbares fTPM durch Remote Attestierung

Author:	Andreas Korb
Supervisor:	Prof. Claudia Eckert
Advisor:	Albert Stark
Submission Date:	15.11.2023

I confirm that this master's thesis is my own work and I have documented all sources and material used.

Munich, 15.11.2023 Andreas Korb

Acknowledgments

Abstract

Contents

1 Introduction

1.1 Motivation

1.2 Goal

1.3 Threat Model

1.4 Environment

1.5 Outline

2 Background

This chapter discusses the relevant background knowledge required to understand the remainder of this work.

2.1 Trusted execution environment

A Trusted execution environment (TEE) is a trusted execution environment on a processor isolated by hardware. It allows code to be executed and data to be stored on a device in a hardware-protected manner that ensures a high level of confidentiality and integrity. One such environment is ARM's TrustZone [1]. It partitions all software and hardware resources of the containing system into the Normal world (NW) and the Secure world (SW). While the SW can access the resources of the SW and the NW, the NW is restricted to its own resources. Since ARM is the dominant processor architectures for IoT devices with a market share of 86 % [2], many of the approaches in this field of research rely on ARM technology such as TrustZone. Our approach also leverages TrustZone to run a trusted application in the SW that monitors the control-flow of the OS kernel in the NW.

2.2 Trusted Platform Module

2.2.1 dTPM

2.2.2 vTPM

2.2.3 fTPM

2.3 Attestation

2.3.1 Local attestation

2.3.2 Remote attestation

Remote attestation is the process initiated by a remote trusted party (called "verifier") to verify that an end-device (called "prover") has not been tampered with. For detecting

that, remote attestation generally inspects the following properties of a program: (i) its code and data has been correctly loaded into memory for execution, (ii) its execution has not been redirected in unintended ways at runtime, and (iii) its data has not been maliciously modified at runtime.

A trusted anchor is required on the device to be attested because at least one trusted component is necessary to extract the data from the remote device to be verified. In many cases, TEE's act as a trust anchor because they are hardware-protected, making it an excellent candidate for a trust anchor.

Abbreviations

TEE Trusted execution environment

List of Figures

List of Tables

Bibliography

[1] ARM Limited. *ARM Security Technology - Building a Secure System using TrustZone Technology*. Issue C. 2009.

[2] E. foundation. *IoT & Edge Developer Survey Report*. (Accessed July 2022). 2022.