SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Thesis title

Andreas Korb

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Thesis title

Titel der Abschlussarbeit

Prof. Claudia Eckert

Author: Andreas Korb

Advisor: Albert Stark Submission Date: 15.11.2023

Supervisor:

I confirm that this master's thesis is my own and material used.	work and I have documented all sources
Munich, 15.11.2023	Andreas Korb



Abstract

Contents

A	cknov	vledgn	nents					111				
Abstract												
1	Intr	oductio	on					1				
	1.1	Section	on					1				
		1.1.1	Subsection				•	1				
2	Bac	kgroun	nd					3				
	2.1	Truste	ed execution environment					3				
	2.2	Truste	ed Platform Module					3				
		2.2.1	dTPM					3				
		2.2.2	vTPM					3				
		2.2.3	fTPM					3				
	2.3	Attest	tation					3				
		2.3.1	Local attestation					3				
		2.3.2	Remote attestation				•	3				
A	bbrev	iations	s					5				
Li	st of	Figures	es ·					6				
Li	st of	Tables						7				
Bi	bliog	raphy						8				

1 Introduction

1.1 Section

Citation test [1].

Acronyms must be added in main.tex and are referenced using macros. The first occurrence is automatically replaced with the long version of the acronym, while all subsequent usages use the abbreviation.

E.g. \ac{TUM} , \ac{TUM} \Rightarrow Technical University of Munich (TUM), TUM For more details, see the documentation of the acronym package¹.

1.1.1 Subsection

See Table 1.1, Figure 1.1, Figure 1.2, Figure 1.3.

Table 1.1: An example for a simple table.

A	В	C	D
1	2	1	2
2	3	2	3

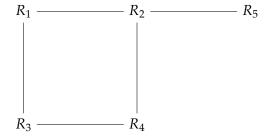


Figure 1.1: An example for a simple drawing.

¹https://ctan.org/pkg/acronym



Figure 1.2: An example for a simple plot.

```
SELECT * FROM tbl WHERE tbl.str = "str"
```

Figure 1.3: An example for a source code listing.

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 [2]. 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% [3], 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

TUM Technical University of Munich

TEE Trusted execution environment

List of Figures

1.1	Example drawing	1
1.2	Example plot	2
1.3	Example listing	2

List of Tables

11	Example table																	- 1
	HVamnia tania																	
1.1	Litallible table																	

Bibliography

- [1] L. Lamport. LaTeX: A Documentation Preparation System User's Guide and Reference Manual. Addison-Wesley Professional, 1994.
- [2] ARM Limited. ARM Security Technology Building a Secure System using TrustZone Technology. Issue C. 2009.
- [3] E. foundation. IoT & Edge Developer Survey Report. (Accessed July 2022). 2022.