JOHANNES KEPLER
UNIVERSITY LINZ

Submitted by
Michael Preisach, BSc
1155264

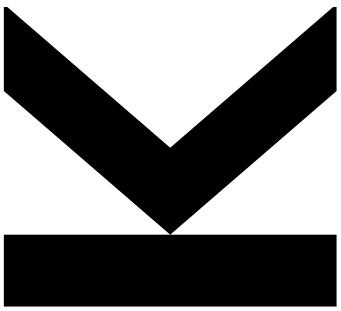
Submitted at
Institute for Networks and Security

Supervisor and First Examiner
Univ.-Prof. DI Dr.
René Mayrhofer

Second Examiner
DI **Tobias Höller**

April 13, 2020

Project Digidow: Biometric Sensor



JOHANNES KEPLER UNIVERSITY LINZ
Altenbergerstraße 69
4040 Linz, Österreich
www.jku.at
DVR 0093696

JOHANNES KEPLER
UNIVERSITY LINZ

Abstract

Zusammenfassung

JOHANNES KEPLER
UNIVERSITY LINZ

Contents

JOHANNES KEPLER
UNIVERSITY LINZ

1 Introduction

All about motivation of doing this masterthesis

- introduction in project digidow
- privacy
- integrity

2 Concept

The theoretical tool that should be formed to one whole system implementation in this thesis

2.1 Attack Vectors and Threat Model

2.2 Trust and Security

2.3 Systems of Trust

2.3.1 Secure Boot, TXT, ...

2.3.2 TPM1.2

2.3.3 TPM2.0

2.4 Verify Trust (DA and DAA)

JOHANNES KEPLER
UNIVERSITY LINZ

3 Handling Biometric Data

3.1 Extend the Trust to External Hardware

3.2 Mitigation of Attack Vectors

4 Implemtentation and Limitations

4.1 Trusted Boot

4.2 Linux Kernel Integrity Tools

5 Conclusion and Outlook

It is yet very hard to implement a system of this kind. The tools are available, but the documentation is not. I did at least figure out what a prototype can look like. Table 5.1 is an example of a table, in which the numbers are aligned at the comma, every second line is colored and the commands `\toprule`, `\midrule` and `\bottomrule` are used [1].

Table 5.1: Example

Länge l in m	Breite b in m	Höhe h in m
12.454	1.24	335.3
543.22	32.123	33.21
353.0	33.0	33.0
23.3	333.2	32.4

JOHANNES KEPLER
UNIVERSITY LINZ

List of Figures

List of Tables

Bibliography

[1] Will Arthur, David Challener, and Kenneth Goldman. *A Practical Guide to TPM 2.0*. Jan. 2015. doi: 10.1007/978-1-4302-6584-9.

1 Installing IMA on Arch

https://wiki.archlinux.org/index.php/Kernel/Arch_Build_System in combination with https://wiki.gentoo.org/wiki/Integrity_Measurement_Architectur

```
sudo pacman -S asp base-devel
cd ~
mkdir build && cd build
asp update linux
asp export linux        #Linux repo exported to this directory
```

Change *pkgbase* in linux/PKGBUILD to custom name, e.g. linux-ima. Check linux/config for the following settings:

```
CONFIG_INTEGRITY=y
CONFIG_IMA=y
CONFIG_IMA_MEASURE_PCR_IDX=10
CONFIG_IMA_LSM_RULES=y
CONFIG_INTEGRITY_SIGNATURE=y
CONFIG_IMA_APPRAISE=y
IMA_APPRAISE_BOOTPARAM=y
```

For optimizing file access, add to every fstab-entry *iversion*. It prevents creating a hash of the file at every access. Instead the hash will only be created when writing the file.

updpkgsums generates new checksums for the modified files.

`makepkg -s` then makes the new kernel