Migration of Secure Enclaves

Master of Science Thesis
University of Turku
Faculty of Technology
Huawei - HERS
2021
Vasile Adrian Bogdan Pop

Supervisors:
Arto Niemi
"Seppo Virtanen"

UNIVERSITY OF TURKU
Faculty of Technology

Vasile Adrian Bogdan Pop: Migration of Secure Enclaves

Master of Science Thesis, 14 p.
Huawei - HERS
October 2021

Keywords: tähän, lista, avainsanoista

Contents

List of Figures

List of Tables

1 Introduction

write stuff because you want write stuff because you want

write stuff because you want write stuff because

you want write stuff because you want write

stuff because you want write stuff because you

want write stuff because you want write stuff

because you want write stuff because you want

write stuff because you want write stuff because

you want write stuff because you want write

stuff because you want write stuff because you want

1.1 Sec 1

2 Background

2.1 Security Principles

2.2 Confidential Computing

2.3 TCB - Trusted Computing Base

2.4 TEE - Truseted Execution Environment

2.5 Remote attestation

3 Secure Enclaves

3.1 State of the Art

3.2 Existing implementation details

3.3 Existing problems with the actual implementations

4 Secure Enclave Migration

4.1 Sec 1

5 Implementation

5.1 Sec 1

6 Conclusions