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"

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

UNIVERSITY OF TURKU
Faculty of Technology

Vasile Adrian Bogdan Pop: Migration of Secure Enclaves

Master of Science Thesis, B-2 p., 4 app. p.
Huawei - HERS
October 2021

Keywords: tähän, lista, avainsanoista

Contents

Appendices

List of Figures

List of Tables

List of acronyms

API Application Programming Interface

UI User Interface

1 Introduction

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

Appendix A Liitedokumentti

Liitteen ohjelmakoodi 1 kuvaa matemaattisen monadirakenteen pohjalta rakentuvan Haskellin tyyppiluokan. Tyyppiluokan voi nähdä eräänlaisena abstraktina ohjelmointirajapintana (API), joka muodostaa ohjelmoijalle abstraktin ohjelmointikielen käyttöliittymän (UI).

Listing 1 Tyyppiluokka 'Monad'.

```
{haskell}

class Monad m where

    ( >>= )         :: m a -> (a -> m b) -> m b

    return          :: a                 -> m a


    fail            :: String            -> m a

    (>>)            :: m a -> m b        -> m b

    m >> k          =  m >>= \_ -> k       -- default


instance Monad IO where  ...               -- omitted
```

Ensimmäisen liitteen toinen sivu. Ohjelmalistaus 2 demonstroi vielä monadin käyttöä.

Listing 2 Monadin käyttöä.

```
{haskell}

main =

return "Your name:" >>=

putStr >>=

\_ -> getLine >>=

\n -> putStrLn ("Hey " ++ n)
```

Appendix B Liitedokumentti 2

Tässä esimerkki

toisesta kaksisivuisesta liitteestä.