Migration of Secure Enclaves

Master Thesis
Turun yliopisto
Tietotekniikan laitos
Huawei
2021
Vasile Adrian Bogdan Pop

Abstract

Sisällys

Kuvat

Taulukot

1 Johdanto

Viittaaminen lukuun 1, toiseen lukuun 2, alilukuun 1.1, tätä alempaan lukuun 1.1.1, alimpaan lukuun 1.1.1, kuvaan 1.1 ja tauluun 1.1.

Kuva liitetään seuraavasti. ShareLaTeXin autocomplete rakentaa koko begin-end blockin yleensä puolestasi.

Taulukkoja tehdään seuraavasti.

Kirjallisuusviitteet lisätään bib-muodossa bibliografia tiedostoon ja niihin viitataan niiden ID:llä, joka on bib-muodon ensimmäinen kenttä **crawley2007write**.

1.1 Alaotsikko

Uskonpuhdistuksen myötä suomi tuli koko jumalanpalveluksen kieleksi. Raamattu ja liturgiset kirjat oli siksi saatava suomeksi. Maahan tarvittiin suomea osaavia pappeja; kouluihin piti sen vuoksi saada suomen kielen opetusta, ja sitä varten tarvittiin oppikirjoja. Nämä asiat olivat nuoren Mikael Agricolan kannustimena, kun hän aloitti elämäntyönsä suomen kirjakielen kehittäjänä.

Agricola opiskeli monen muun suomalaisnuorukaisen tavoin Wittenbergissä. Jo

Kuva 1.1: Kuvan otsikko

Taulukko 1.1: Taulukon otsikko tulee taulun yläpuolelle

Taulun	elementit	erotetaan
toisistaan	et-merkillä	
soluja voi myös		jättää tyhjäksi

ennen Wittenbergin vuosia hän oli saanut valmiiksi Abckirian ja Rucouskirian. Abckiria oli tarkoitettu oppikirjaksi. Se sisälsi aakkoset, tavausharjoituksia ja katekismuksen. Laajassa Rucouskiriassa on rukousten lisäksi Raamatun tekstejä, muun muassa 41 psalmia. Alussa on monipuolinen kalendaario, joka sisältää esimerkiksi ruokailu- ja terveydenhoito-ohjeita ja jopa jonkinlaisen horoskoopin.

Uutta testamenttia Agricola käänsi Wittenbergissä apuneuvoinaan kaksi latinalaista, kaksi saksalaista ja kaksi ruotsalaista käännöstä. Se Wsi Testamenti ilmestyi 1548. Kirjan sanasto ja muoto-oppi on siinä määrin epäyhtenäistä, että on arveltu, että käännöksellä on Agricolan lisäksi ollut myös muita viimeistelijöitä.

Agricolan osuus 1551 ilmestyneen Psalttarin psalmisuomennoksista on epäselvä. Suuri osa psalmeista onkin todennäköisesti suomennettu Turun koulussa Paavali Juustenin johdolla. Juusten itse on kirjoittanut Psalttarista Suomen piispainkronikassa (suom. Simo Heininen): “Mutta ei ole ollenkaan väliä, kenen nimissä se on julkaistu, sillä se on käännetty, jotta siitä olisi suurta hyötyä Suomen kansalle.” Pääosa Psalttarin esipuheista on Agricolan omaa tekstiä. Runomuotoiseen esipuheeseen sisältyy ansiokas luettelo suomalaisten pakanallisista jumalista. Agricola suomensi myös osia Mooseksen kirjoista ja profeetoista. Hänen nimissään on ilmestynyt suomeksi noin 2/5 Raamatusta.

Toinen esimerkki viittaamisesta, jossa myös cite-komennon tagi löytyy tiedostosta Bibliografia.bib **puasuareanu2009survey**.

1.1.1 Alempiotsikko

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam eget tellus porttitor, tempus lacus non, pellentesque ligula. Donec sit amet erat condimentum, feugiat mi accumsan, euismod quam.

Mauris laoreet maximus aliquet. Mauris at gravida elit. Ut nec lobortis elit. Sed lacinia nisi in ex sollicitudin, ac consequat lacus imperdiet. Etiam et velit eu lacus maximus faucibus.

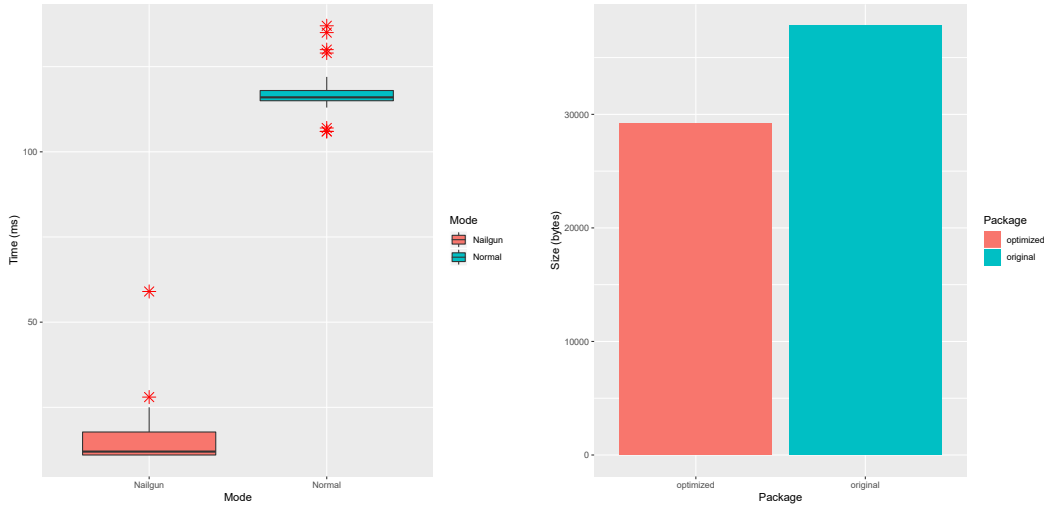
Alinotsikko, joka ei näy sisällysluettelossa

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam eget tellus porttitor, tempus lacus non, pellentesque ligula. Donec sit amet erat condimentum, feugiat mi accumsan, euismod quam.

Otsikko tekstissä, joka ei näy sisällysluettelossa Mauris laoreet maximus aliquet. Mauris at gravida elit. Ut nec lobortis elit. Sed lacinia nisi in ex sollicitudin, ac consequat lacus imperdiet. Etiam et velit eu lacus maximus faucibus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Donec vulputate tellus ullamcorper odio sodales, non scelerisque neque eleifend.

2 Toisen luvun otsikko

Tässä luvussa tarkastellaan kahden kuvan upottamista samaan kelluvaan kuvaympäristöön (Kuva 2.1).



(a) Käynnistysajan optimointi Nailgunilla.

(b) Koon optimointi Proguardilla.

Kuva 2.1: Optimointia kahdella eri tavalla.

3 Introduction

3.1 Sec 1

4 Background

4.1 Security Principles

4.2 Confidential Computing

4.3 TCB - Trusted Computing Base

4.4 TEE - Truseted Execution Environment

4.5 Remote attestation

5 Secure Enclaves

5.1 State of the Art

5.2 Existing implementation details

5.3 Existing problems with the actual implementations

6 Secure Enclave Migration

6.1 Sec 1

7 Implementation

7.1 Sec 1

8 Conclusions

Liite 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).

Ohjelmalistaus 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.

Ohjelmalistaus 2 Monadin käyttöä.

```
{haskell}

main =

return "Your name:" >>=

putStr >>=

\_ -> getLine >>=

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

Liite B Liitedokumentti 2

Tässä esimerkki

toisesta kaksisivuisesta liitteestä.