VICTORIA UNIVERSITY OF WELLINGTON
Te Whare Wānanga o te Ūpoko o te Ika a Māui

School of Engineering and Computer Science
Te Kura Mātai Pūkaha, Pūrorohiko

PO Box 600
Wellington
New Zealand

Tel: +64 4 463 5341
Fax: +64 4 463 5045
Internet: office@ecs.vuw.ac.nz

Cloud Key Management

Sriram Venkatesh

Supervisor: NOT STATED

Submitted in partial fulfilment of the requirements for
Master of Computer Science.

Abstract

A short description of the project goes here.

Acknowledgments

Any acknowledgments should go in here, between the title page and the table of contents. The acknowledgments do not form a proper chapter, and so don't get a number or appear in the table of contents.

Contents

Figures

Chapter 1

Introduction

~~This chapter gives an introduction to the project report.~~

1.1 Motivation

1.2 Problem

1.3 Contributions

Chapter 2

Background

2.1 ~~System Security~~

2.1 ~~Cryptography~~Security System

2.2 ~~Authentication and Authorization Protocols~~

2.1.1 What defines a secure system?

2.1.2 Cryptography

2.1.3 Trust

2.1.4 Authentication

2.1.5 Authorization

2.1.6 Access Control

2.2 Key Management

2.2.1 What is Key Management?

2.2.2 Importance of Key Management

2.2.3 Public Key Infrastructures

2.3 ~~Trust Management Systems~~

2.2.1 ~~Kerberos~~

2.3 ~~Threat Modeling~~

2.2.1 ~~OWASP Threat Modeling Technique~~

2.2.1 ~~Microsoft Threat Modeling Technique~~

2.3 Defining the Cloud

2.3.1 Cloud Service Models

2.3.2 Security in the Cloud

2.4 Vendors

2.4.1 Amazon Web Services

2.4.2 Luna SA

Chapter 3

~~Traditional Use Case~~Problem Domain

3.1 Description of Baseline model

3.2 ~~Decoupling the application~~Threat Modeling

3.2.1 OWASP Threat Modeling Technique

3.2.2 ~~Application Components~~

3.3 Application Architecture

3.3.1 User Roles

3.4 ~~Interaction between different components~~

3.3.1 Key Retrieval

3.3.2 ~~Running Application~~Key Bootstrapping

3.4 Trust Model~~Assumptions~~

3.4.1 Application Assumptions

3.4.2 Power of attacker

3.5 Threat Scenario Evaluation

3.5.1 Threat Analysis

3.5.2 Threat Matrix

Chapter 4

~~Threat Model Analysis~~Possible Solutions

4.1 Eso

4.1.1 What is Eso?

4.1.2 System Process

4.1.2.1 Key Retrieval

4.1.2.2 Key Bootstrapping Process

4.1.2.3 Key Revocation

4.1.3 Security Analysis

4.1.3.1 System Threats

4.1.3.2 Threat Model Evaluation

4.2 HSM

4.2.1 What is HSM?

4.2.2 System Process

4.2.3 Architectural Overview

4.2.3.1 Key Retrieval

4.2.3.2 Key Bootstrapping Process

4.2.3.3 Key Revocation

4.2.4 Security Analysis

4.2.4.1 System Threats

4.2.4.2 Threat Model Evaluation

4.3 SoftHSM

4.3.1 What is SoftHSM?

4.3.2 System Process

4.3.3 Architectural Overview

4.3.3.1 Key Retrieval

4.3.3.2 Key Bootstrapping Process

4.3.3.3 Key Revocation

4.3.4 Security Analysis

4.3.4.1 System Threats

4.3.4.2 Threat Model Evaluation

4.4 ~~Security Matrix Comparison~~

Chapter 5

Implementation

5.1 Program Architecture

5.1.1 Scenario

5.1.2 High Level Overview

5.1.3 Process Overview

5.1.4 Key Bootstrap Process

5.1.5 Key Retrieval Process

5.1.5.1 Credential Storage

5.1.5.2 Design

5.2 Experimental Design

5.2.1 Performance Metrics

5.2.2 Comparison with traditional use case

Chapter 6

Evaulation

6.1 Security Threat Matrix Evaluation

6.2 Results and Findings

6.2.1 Security Analysis

6.2.2 Performance Tests and Comparaison

6.3 Costing Analysis

Chapter 7

Conclusions

The conclusions are presented in this Chapter.

Bibliography