**Abstract**

This is the abstract for my master's thesis.

## Copyright

## Disclaimer

## Acknowledgements

# Table Of Contents


Abstract . . . . . 4

**List of Figures** **5**

**List of Tables** **5**

List of Acronyms . . . . . 5

**1 Introduction** **7**

**2 Background** **8**

**3 Systems Security Engineering** **9**

3.1 NIST Special Publication 800-160 . . . . . 9

3.2 Verification & Documentation . . . . . 9

3.3 Principle of Complete Mediation . . . . . 9

3.3.1 Formal Verification Using Computer-Aided Reasoning . 9

**4 Certified Security by Design (CSBD) & Access-Control Logic (ACL)** **10**

4.1 Certified Security by Design (CSBD) . . . . . 11

4.2 Access-Control Logic (ACL) . . . . . 11

4.2.1 Principals . . . . . 11

4.2.2 Well-formed Formulas Formulas . . . . . 11

4.2.3 Kripke Structure . . . . . 11

4.2.3.1 satisies . . . . . 11

4.2.3.2 soundness . . . . . 11

4.2.4 Well formed statements . . . . . 11

4.2.5 Inference Rules . . . . . 11

4.2.6 Complete mediation . . . . . 11

4.3 ACL in HOL . . . . . 11

4.3.1 satList . . . . . 11

4.3.2 Complete Mediation . . . . . 11

**5 Patrol Base Operations** **12**
5.1 Motivation . . . 13
5.2 Ranger Handbook Description . . . 13
5.3 Describing The Patrol Base Operations . . . 13
5.4 Hierarchy of Secure State Machines . . . 13
5.4.1 OMNI-Level . . . 13
5.4.2 Escape . . . 13
5.4.3 Top Level . . . 13
5.4.4 Horizontal Slice . . . 13
5.4.4.1 ssmPlanPB . . . 13
5.4.4.2 ssmMoveToORP . . . 13
5.4.4.3 ssmConductORP . . . 13
5.4.4.4 ssmMoveToPB . . . 13
5.4.4.5 ssmConductPB . . . 13
5.4.5 Vertical Slice . . . 13
5.4.5.1 ssmSecureHalt . . . 13
5.4.5.2 ssmORPRecon . . . 13
5.4.5.3 ssmMoveToORP4L . . . 13
5.4.5.4 ssmFormRT . . . 13

**6 Secure State Machine Model** **14**
6.1 State Machines . . . 15
6.1.1 Next-state Function . . . 15
6.1.2 Next-output Function . . . 15
6.1.3 Transition Commands . . . 15
6.2 Secure State Machines . . . 15
6.2.1 State Machine Versus Secure State Machine . . . 15
6.2.2 Transition Types . . . 15
6.2.3 Authentication . . . 15
6.2.4 Authorization . . . 15
6.3 Secure State Machines in HOL . . . 15
6.3.1 Parameterizable Secure State Machine . . . 15
6.3.2 Parameterization . . . 15
6.3.3 Configurations: five parts . . . 15
6.3.3.1 State Interpretation . . . 15
6.3.3.2 Security context . . . 15
6.3.3.3 Input stream . . . 15
6.3.3.4 State . . . 15
6.3.3.5 Output stream . . . 15
6.3.4 Authentication . . . 15
6.3.5 Configuration Interpretation . . . 15

6.3.6 Transition Definitions . . . . . 15

**7 Patrol Base Operations as Secure State Machines 16**
7.1 ssmPB: An Example from the Hierarchy . . . . . 16
7.1.1 Principals . . . . . 16
7.1.2 States . . . . . 16
7.1.3 Commands . . . . . 16
7.1.4 Next-State Function . . . . . 16
7.1.5 Next-Output Function . . . . . 16
7.1.6 Authentication . . . . . 16
7.1.7 Authorization . . . . . 16
7.1.8 Proved Theorems . . . . . 16
7.1.8.1 Platoon Leader Is Trusted on plCommands . 16
7.2 Other Variations . . . . . 16
7.2.1 ssmPlanPB: Non-sequential Transitions . . . . . 16
7.2.2 ssmConductORP: Principals Authorized for Subsets of Commands . . . . . 16

**8 Discussion 17**
8.1 Recap . . . . . 17
8.2 Mission Accomplished . . . . . 17
8.3 Stop-Gaps, Lessons Learned, & Advice . . . . . 17
8.4 Other Verifiable Theories . . . . . 17
8.4.1 Platoon Theory, Soldier Theory, Squad Theory, etc. . . 17
8.4.2 Soldiers in Roles . . . . . 17

**9 Future Work & Implications 18**
9.1 The Devil Is in The Details . . . . . 18
9.2 Accountability Systems . . . . . 18
9.3 Applicability . . . . . 18

**10 Appendices 19**
.1 Access Control Logic Theories in HOL . . . . . 19
.2 Secure State Machine Theories Applied to Patrol Base Operations . . . . . 19
.3 Pretty-Printed Theories . . . . . 19
.4 Map of The File Folder Structure . . . . . 19

# List of Figures

# List of Tables

## List of Acronyms

# Chapter 1

# Introduction

# Chapter 2

# Background

### Formal Methods

### Functional Programming

### Higher Order Logic (HOL) Interactive Theorem Prover

### Other Interactive Theorem Provers

# Chapter 3

# Systems Security Engineering

## 3.1 NIST Special Publication 800-160

## 3.2 Verification & Documentation

## 3.3 Principle of Complete Mediation

### 3.3.1 Formal Verification Using Computer-Aided Reasoning

# Chapter 4

# Certified Security by Design (CSBD) &

# Access-Control Logic (ACL)

## 4.1 Certified Security by Design (CSBD)

## 4.2 Access-Control Logic (ACL)

### 4.2.1 Principals

### 4.2.2 Well-formed Formulas Formulas

### 4.2.3 Kripke Structure

#### 4.2.3.1 satisies

#### 4.2.3.2 soundness

### 4.2.4 Well formed statements

### 4.2.5 Inference Rules

### 4.2.6 Complete mediation

## 4.3 ACL in HOL

### 4.3.1 satList

### 4.3.2 Complete Mediation

# Chapter 5

# Patrol Base Operations

## 5.1 Motivation

## 5.2 Ranger Handbook Description

## 5.3 Describing The Patrol Base Operations

## 5.4 Hierarchy of Secure State Machines

### 5.4.1 OMNI-Level

### 5.4.2 Escape

### 5.4.3 Top Level

### 5.4.4 Horizontal Slice

#### 5.4.4.1 ssmPlanPB

#### 5.4.4.2 ssmMoveToORP

#### 5.4.4.3 ssmConductORP

#### 5.4.4.4 ssmMoveToPB

#### 5.4.4.5 ssmConductPB

### 5.4.5 Vertical Slice

#### 5.4.5.1 ssmSecureHalt

#### 5.4.5.2 ssmORPRecon

#### 5.4.5.3 ssmMoveToORP4L

#### 5.4.5.4 ssmFormRT

# Chapter 6

# Secure State Machine Model

## 6.1 State Machines

### 6.1.1 Next-state Function

### 6.1.2 Next-output Function

### 6.1.3 Transition Commands

## 6.2 Secure State Machines

### 6.2.1 State Machine Versus Secure State Machine

### 6.2.2 Transition Types

### 6.2.3 Authentication

### 6.2.4 Authorization

## 6.3 Secure State Machines in HOL

### 6.3.1 Parameterizable Secure State Machine

### 6.3.2 Parameterization

### 6.3.3 Configurations: five parts

#### 6.3.3.1 State Interpretation

#### 6.3.3.2 Security context

#### 6.3.3.3 Input stream

#### 6.3.3.4 State



#### 6.3.3.5 Output stream

### 6.3.4 Authentication

### 6.3.5 Configuration Interpretation

### 6.3.6 Transition Definitions

# Chapter 7

# Patrol Base Operations as Secure State Machines

## 7.1 ssmPB: An Example from the Hierarchy

### 7.1.1 Principals

### 7.1.2 States

### 7.1.3 Commands

### 7.1.4 Next-State Function

### 7.1.5 Next-Output Function

### 7.1.6 Authentication

### 7.1.7 Authorization

### 7.1.8 Proved Theorems

#### 7.1.8.1 Platoon Leader Is Trusted on plCommands

## 7.2 Other Variations

### 7.2.1 ssmPlanPB: Non-sequential Transitions

### 7.2.2 ssmConductORP: Principals Authorized for Subsets of Commands

# Chapter 8

# Discussion

## 8.1 Recap

## 8.2 Mission Accomplished

## 8.3 Stop-Gaps, Lessons Learned, & Advice

## 8.4 Other Verifiable Theories

### 8.4.1 Platoon Theory, Soldier Theory, Squad Theory, etc.

### 8.4.2 Soldiers in Roles

# Chapter 9

# Future Work & Implications

## 9.1 The Devil Is in The Details

## 9.2 Accountability Systems

## 9.3 Applicability

# Chapter 10

# Appendices

## .1 Access Control Logic Theories in HOL

## .2 Secure State Machine Theories Applied to Patrol Base Operations

## .3 Pretty-Printed Theories

## .4 Map of The File Folder Structure

# Bibliography