An Interaction-based Software-Defined Security Model and Platform to secure cloud resources

A dissertation submitted to

Faculty of Engineering and Information Technology

University of Technology Sydney

In fulfilment of the requirements for the award of

Doctor of Philosophy

By

Sara Farahmandian

Supervised by

Professor Doan B. Hoang

2021

Dedicated To

My Divine Source

My parents, and my siblings

My primary supervisor

Thank for your great support and love

Certificate of Original Authorship

I, Sara Farahmandian declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the Faculty of Engineering and Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature of Student: Sara Farahmandian

Production Note:
Signature removed prior to publication.

Date: <04/01/2021>

Acknowledgement

During my doctoral candidature, I have received a myriad of lessons, support, and encouragement. I wish to express my sincere gratitude to my supervisor, Professor Doan B. Hoang, for his support and for sharing this journey alongside me. I cannot express in words how grateful I am and how much his supervision and mentorship meant to me. He has taught me significantly valuable lessons that enlightened my academic and personal life. He has been outstanding in providing insightful feedback and creating the balance between working and living. Following his lessons, I gradually become an independent researcher. I would like to thanks my co-supervisor, Dr. Priyadarsi Nanda, for his support during my candidature.

I am thankful for all SEDE staff who supports me in every steps of my journey. I would like to express my special thanks to all my teammates and friends in UTS Women in Engineering and IT (WiEIT) for their remarkable help and support. I will never forget the encouragement and assistance from all my colleagues and friends, including Tham Nguyen, Chau Nguyen, Ngoc Le, Tuan Vinh Ha, Hasti Hayati, Behnam Maleki, Ashish Nanda, Madhumita Abhijeet Takalkar, Deepak Puthal, Marie Joshua Tapas, and Azita Zoughi.

Finally, I would like to show my appreciation to my Family. To my mother, Parvin, the most incredible light in my life who taught me to be kind and strong and supported me in every hard steps of my life, to my father who always encourage me to overcome difficulties in my life, to my sister, Sepideh, who is my role model and symbol of pure light and love in my life, to my wonderful brother, Ehsan, whom talking to always keep me motivated, to my sister-in-law, Azadeh, who always kindly supported and encouraged me during this journey, to my little niece, Elina, whom her existence brings me pure joy and happiness, to my brother, Amin, whom always encouraged me in every step of life. Their support and love encouraged me in every step of my journey. This dissertation is dedicated to them. Without all of you, this research journey would not have been possible.

Author’s Publications

Journal Article:

1. Hoang, D.B. and **S. Farahmandian**, *“Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies”,* in Guide to Security in SDN and NFV. 2017. Springer. p. 3-32.

2. **Farahmandian, S**. and D.B. Hoang, *“Policy-based Interaction Model for Cloud Security Breaches Detection and Prediction”*. Journal of Telecommunications and the Digital Economy, 2020.

3. **Farahmandian, S.** and D.B. Hoang, *“Software-defined Security Service Platform for Securing Cloud Infrastructure”*. IEEE Transactions on Cloud Computing (TCC) Journal, 2021 (under-review).

Conference Papers:

4. **Farahmandian, S**. and D.B. Hoang. *Security for software-defined (cloud, SDN and NFV) infrastructures–issues and challenges.* in Eight international conference on network and communications security. 2016.

5. **Farahmandian, S**. and D.B. Hoang. *SDS 2: A novel software-defined security service for protecting cloud computing infrastructure*. in 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). 2017. IEEE.

6. **Farahmandian, S**. and D.B. Hoang. *A Policy-based Interaction Protocol between Software Defined Security Controller and Virtual Security Functions.* in 2020 4th Cyber Security in Networking Conference (CSNet). 2020. IEEE.

Table of Contents

Certificate of Original Authorship 2
Acknowledgement 3
Author's Publications 4
Table of Contents 5
Figures 9
Tables 15
Algorithms 15
Abbreviations and Acronyms 16
Abstract 18
Chapter 1 Introduction 20
1.1 Introduction 20
1.2 Brief Background 26
1.2.1 Software-Defined Infrastructure paradigm 27
1.2.2 Software-Defined Security (SDSec) 28
1.2.3 Software-Defined Security Service (SDS_2) 30
1.2.4 Software-Defined Network of Virtual Security Functions 31
1.2.5 Provision of software-based security functions on-demand 31
1.2.6 Security Issues and Challenges in an Integrated Cloud/SDN/NFV Infrastructure Platform 32
1.3 Research Questions 34
1.4 Research Aim and Objectives 37
1.5 Research Contributions and Significance 38
1.6 Research Methodology 40
1.7 Thesis Structure 42
Chapter 2 Background and Related Work 46
2.1 Introduction 46
2.2 Software-Defined Infrastructure 47
2.2.1 Virtualization 48
2.3 Cloud Computing 57
2.3.1 Cloud terminology – roles and boundaries 60
2.3.2 Cloud Security 62
2.4 Software-Defined Networking 67
2.4.1 SDN Interfaces 69
2.4.2 SDN Security Challenges 72
2.5 Network Function Virtualization 76

2.5.1 NFV Security Challenges 80
2.6 Policy 82
2.6.1 Security Policy Mechanisms 86
2.6.2 Access Control Policy Enforcement Methods 87
2.7 Security by Isolation 90
2.7.1 Isolation Classification 91
2.7.2 Standard Network Security Solutions by Isolation 93
2.7.3 Cloud resource isolation mechanisms 94
2.8 Open-sources for Deploying a Cloud Security SDN/NFV platform95
2.9 Summary 96
Chapter 3 Software-Defined Security Service Model 97
3.1 Introduction 97
3.2 Why Programmable and automated Security Services on Demand? 98
3.3 Software-Defined Security Service (SDS_2) Model 102
3.3.1 SDS_2 Security Layers 105
3.4 Application of SDS_2 to Data Centre Security 108
3.5 SDS_2 Features 109
3.6 Thesis Roadmap 113
3.7 Summary 115
Chapter 4 SDS_2 Policy-based Interaction Model for Cloud Security Breaches detection and Prediction 116
4.1 Introduction 116
4.2 Cloud Object Model used for Interaction Model 117
4.3 Interaction Model 121
4.3.1 Interaction Mode 124
4.3.2 Interaction Positional Relationship (R) 125
4.3.3 Interaction time (t) 126
4.3.4 Interaction Action (A) 126
4.4 Security Policy-Based Interaction Model 128
4.5 Interaction Security Violation Detection and Prediction Algorithm (ISVDP) 133
4.5.1 Interaction Security Violation Detection 136
4.5.2 Interaction Security Violation Prediction 138
4.6 Interaction scenarios and results 140
4.7 Summary 149
Chapter 5 Sec-MANAGE Protocol 150
5.1 Introduction 150
5.2 Software-Defined Security Service (SDS_2) and Interaction Model 151
5.2.1 SDS_2 Security Controller 153

5.2.2 SDS$_2$ Policy-based Interaction Model 154
5.3 Sec-Manage Protocol Design 156
5.3.1 Sec-Manage packet header 158
5.3.2 Message types 159
5.3.3 Forwarding Interaction Table Specification 162
5.3.4 Config Interaction Table Specification 164
5.4 Implementation and Performance Evaluation 166
5.4.1 Implementation Set up 166
5.4.2 Performance Evaluation 168
5.5 Summary 171
Chapter 6 Software-Defined Security Service Architecture and Components 172
6.1 Introduction 172
6.2 Software-Defined Security Service (SDS$_2$) Architecture 174
6.2.1 Virtual Security Function (VSF) 177
6.2.2 Sec-Manage Protocol 178
6.2.3 Policy-based Interaction Model 178
6.2.4 SDS$_2$ Security Controller 179
6.3 SDS$_2$ Security controller – Functioning Mechanism 182
6.3.1 Virtual Security Function orchestration approach 182
6.3.2 VSF Configuration Approach 183
6.4 SDS$_2$ Security Controller – Software Implementation 184
6.5 Results and Performance evaluation 186
6.5.1 Implementation Set Up 187
6.5.2 SDS$_2$ Security controller - Performance Evaluation 188
6.6 Summary 194
Chapter 7 Software-Defined Security Service Platform 195
7.1 Introduction 195
7.2 Integrated Software-Defined Security architecture 197
7.3 SDS$_2$ Platform – Procedure of provisioning on-demand Security Services to Protect Cloud Resources 202
7.4 SDS$_2$ Platform Implementation 206
7.4.1 Implemented Platform 206
7.4.2 Implementation Scenarios and Results 209
7.4.3 SDS$_2$ Platform setup 222
7.5 SDS$_2$ Platform Performance Evaluation 223
7.5.1 SDS$_2$ platform capability 223
7.5.2 SDS$_2$ platform – Performance 230
7.6 Summary 236

Chapter 8 Conclusion and Future Work 238

8.1 Research Remarks 238

8.2 Future Work.. 243

Bibliography 246

Figures

Figure 1.1 Research Phases 41

Figure 1.2 Research Methodology.. 42

Figure 1.3 Research Structure.. 43

Figure 2.1 Virtual Machines Virtualization.. 50

Figure 2.2 Virtualization Reference Model [35] 53

Figure 2.3 Classification of attacks [35].. 54

Figure 2.4 Security Vulnerabilities and Risk in a Virtual Environment [36] .. 55

Figure 2.5 Cloud provider—three-layer service orchestration model 59

Figure 2.6 Cloud computing front and back end [41]..................................... 60

Figure 2.7 different actors in cloud infrastructure [42] 62

Figure 2.8 SDN Components... 69

Figure 2.9 OpenFlow Switch- operation [53]... 71

Figure 2.10 NFV architecture 77

Figure 2.11 NFV-MANO architectural framework [86] 78

Figure 2.12 Simple Policy {Kosiur, 2001 #163}.. 84

Figure 2.13 A comparison between different types of access control models[117].. 88

Figure 2.14 CCACSM architecture [119] 89

Figure 3.1 SDS_2 overall architecture 105

Figure 3.2 SDS_2 Security Layers 106

Figure 3.3 Security Control Layer 107

Figure 3.4 Security Data Layer 108

Figure 4.1 Cloud Object domain parameters 120

Figure 4.2 Interaction Types 123

Figure 4.3 Interaction Mode 125

Figure 4.4 Security policy and its components 129

Figure 4.5 Security Policy-Based Interaction Model 130

Figure 4.6 Security Isolation levels 132

Figure 4.7 ISVDP stages 134

Figure 4.8 ISVD 137

Figure 4.9 Implementation process 141

Figure 4.10 Extracting involved objects and assigning a monitoring security function to each interaction 143

Figure 4.11 The controller interface according to interaction 144

Figure 4.12 Implementation results for VM-Storage interaction 146

Figure 4.13 Performance monitoring according to interaction detection processing time 148

Figure 4.14 Overview of SDS$_2$ interaction classes 148

Figure 5.1 SDS$_2$ three layers 153

Figure 5.2 SDS$_2$ Security controller and Sec-Manage protocol 154

Figure 5.3 Interaction and Sec-Manage Protocol 156

Figure 5.4 Connection establishment.. 157

Figure 5.5 Sec-Manage Header and payload 158

Figure 5.6 Sec-Manage Protocol Header 159

Figure 5.7 Sec-Manage message types 160

Figure 5.8 Interaction Forward table structure 163

Figure 5.9 Interaction Config Table 165

Figure 5.10 Interaction configuration table class of diagram 165

Figure 5.11 The implementation of the prototype 167

Figure 5.12 Client sending request to the security controller 168

Figure 5.13 Current Service Table... 169

Figure 5.14 Security controller service table after receiving an interaction .. 169

Figure 5.15 VSF Config Table before 170

Figure 5.16 VSF Config table after configuration 170

Figure 5.17 Current VSF forwarding table... 170

Figure 5.18 VSF Forwarding table after configuration 170

Figure 5.19 SDS_2 GUI interface demonstrating multiple interaction forwarding and configuration records 171

Figure 6.1 SDS_2 Layers 173

Figure 6.2 SDS_2 Architecture overview 175

Figure 6.3 overview on SDS_2 major components 180

Figure 6.4 Class Diagram of SDS_2 Security Controller 185

Figure 6.5 Implementation Prototype 187

Figure 6.6 multiple interactions handled by the security controller 189

Figure 6.7 Status of VSFs 190

Figure 6.8 SDS_2 security controller the average processing time for all types of interactions 192

Figure 6.9 Provisioning On-demand security services 193

Figure 7.1 Overview of SDS_2 Layers and components 196

Figure 7.2 Conceptual structure of SDS_2 in an integrated Cloud/SDN/NFV 199

Figure 7.3 Overall SDS_2 security platform workflow 201

Figure 7.4 Workflow of security Network structure 202

Figure 7.5 Overall process of provisioning on-demand security services via SDS_2 204

Figure 7.6 Overview of SDS_2 security controller workflow 205

Figure 7.7 Overview of VSF workflow 206

Figure 7.8 overall view of Platform structure 208

Figure 7.9 SDS_2 service Implementation Scenario..210

Figure 7.10 Overall state of threat Scenario 211

Figure 7.11 Assigned VSF to interactions...212

Figure 7.12 Process time by VSFs..213

Figure 7.13 Violation detection of Int6 213

Figure 7.14 performed tests with two sets of interaction conditions (A*, R*) 214

Figure 7.15 Processing average detection and prediction time for Case 1 and 2 215

Figure 7.16 Captured requested interaction and their policies 216

Figure 7.17 Changes of policies for...217

Figure 7.18 Workflow of VSF no-policy process..218

Figure 7.19 No-policy case- a) demonstrates VSF discovery of interaction with no assigned P.ID, b) presents the new P.ID for interaction, c) shows process time of orchestrating a new policy for particular interaction in two main scenarios 219

Figure 7.20 The SDS_2 platform deals with policy changes during an interaction 219

Figure 7.21 Presents the experiment prototype 220

Figure 7.22 Presents various interaction types 221

Figure 7.23 Presents the assigned PID according to each entity (Src., Dst.). 225

Figure 7.24 Dynamic changes of Policies 226

Figure 7.25 SDS_2 automatically initiates VSFs to monitor interactions........226

Figure 7.26 demonstrates result after SDS_2 runs ISVDP algorithms: a) shows results of ISVD algorithm for various simulated interactions within the system, b) presents results after running ISVP algorithm 227

Figure 7.27 SDS_2 security functions.. 229

Figure 7.28 SDS_2 time diagram 230

Figure 7.29 Orchestration time Case 1 and Case 2.. 232

Figure 7.30 Non-Smart SDS_2 service 233

Figure 7.31 Smart SDS_2 service 234

Figure 7.32 SDS_2 service - performance improvement 235

Figure 7.33 SDS_2 service performance evaluation - in case of different simulated interactions 236

Tables

Table 2.1 Security Vulnerabilities of NFV 81

Table 4.1 Summary of Notations 122

Table 4.2 Action Description 127

Table 4.3 Required Notations 132

Table 4.4 Operations Defined on an Interaction Object 134

Table 4.5 Collected data from the controller for VM-Storage interaction 145

Table 4.6 Expected results of the simulated scenarios 147

Table 6.1 Security Controller VSF Orchestration Results 191

Table 7.1 Main Implemented Components of The Platform 207

Table 7.2 Tested cases 214

Table 7.3 Experiment scenarios 220

Algorithms

Algorithm 4.1 Policy-driven interaction algorithm (PdI ()) 135

Algorithm 4.2 Interaction Security Violation Detection (ISVD ()) algorithm 138

Algorithm 4.3 Interaction Security Violation Detection (ISVD ()) algorithm 139

Algorithm 6.1 VSF Creation.. 183

Algorithm 6.2 Association Requested interaction 184

Abbreviations and Acronyms

NIST	National Institute of Standards and Technology
IEEE	Institute of Electrical and Electronics Engineers
ONF	Open Networking Foundation
ETSI	European Telecommunications Standards Institute
NFV	Network Function Virtualization
SDN	Software-Defined Networking
SDS_2	Software Defined Security Service
OT	Operational technology
SDSec	Software-Defined Security
VNF	Virtual Network Function
EM	Element Management
VSF	Virtual Security Function
VN	Virtual Network
VM	Virtual Machine
SDI	Software-Defined Infrastructure
SDC	Software-Defined compute
SDS	Software-Defined Storage
SC	Security Controller

OS	Operating System
CSA	Cloud Security Alliance
VLAN	Virtual Local Area Network
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SaaS	Software-as-a-Service
PaaS	Platform-as-a-Service
IaaS	Infrastructure-as-a-Service
CP	Cloud Provider
CS	Cloud Service
CSP	Cloud Service Provider
ISP	Infrastructure Service Provider
SLA	Service Level Agreement
API	Application Programming Interface
SSL	Secure sockets layer
TLS	Transport Layer Security
APT	Advanced Persistent Threats
DoS	Denial-of-service
DDoS	Distributed Denial-of-service
SBI	Southbound Interface
NBI	Northbound Interface
OvS	OpenvSwitch
NFVI	NFV Infrastructure
EPC	Evolved Packet Core
MANO	Management and Orchestration
VNFM	Virtual Network Function Manager
VSFM	Virtual Security Function Manager
CC	Cloud Controller
SC	Security Controller
SP	Security Policy
IP	Internet Protocol
MAC	Media Access Control
SPM	Security Policy Manager
ESPM	Entity security policy-driven manager
PIM	Policy-based interaction manager
DPI	Deep Packet Inspections
SNM	Security Network Manager
ID	Identification

Abstract

Cloud computing has transformed a large portion of the IT industry through its ability to provision infrastructure resources – computing, networking, storage, and software – as services. Transferring to such an infrastructure relies on virtualization and its dynamic construction ability to spread over a geographical area. The challenge is in finding effective mechanisms for isolating security issues in cloud infrastructure. Isolation implies creating security boundaries for protecting cloud assets at different levels of a cloud security architecture. Building security boundaries is critical not only for recognizing security violations but also for creating security solutions. However, it is challenging as virtual boundaries are not as clear-cut as physical boundaries in traditional infrastructure. The difficulty rises as virtual boundaries among components are not well defined and often undefined, and hence they are not visible/controllable by the providers.

Additionally, defining object boundaries is extremely difficult because virtual objects are dynamic in both characteristics and functionality. Many efforts have been made to address security isolation challenges, but no attempt has been made to consider an overall solution to a dynamic, intelligent, programable, and on-demand security isolation system. Moreover, there is no platform/framework to deliver programmable and on-demand construction of security boundaries to protect cloud resources.

We develop a new method to protect cloud infrastructure with new intelligent isolation mechanisms to detect and predict security breaks. This research applies promising new technologies, including software-defined networking and network function virtualization, in providing on-demand security services over large-scale cloud infrastructure and overcoming challenges in constructing dynamic security boundaries. To protect cloud resources, we propose a Policy-based Interaction Model

and develop the Software-Defined Security Service. We develop a novel intelligent security isolation interaction algorithm to model security boundaries. To do so, we proposed a Policy-driven Interaction Model to construct dynamic security boundaries intelligently. A Software-Defined Security Service (SDS_2) model was developed with three novel components, including security controller, Sec-Manage protocol, and the virtual security function. The SDS_2 carries the concepts of a logically centralized security controller to provision on-demand security services.

The research novelty lies in its innovative and intelligent security isolation interaction model, novel approach in detecting and predicting security violations, and constructing dynamic, programmable, and on-demand VSFs. It enables i) overall visibility on security boundaries within the cloud infrastructure, ii) the automation of provisioning security services on-demand, iii) a proactive security technique against security interaction violations, iv) separation of security services for both cloud providers and tenants.