A Novel Capability Maturity Model with Quantitative Metrics for Securing Cloud Computing

A thesis submitted in fulfilment of the requirements for
the degree of Doctor of Philosophy
in the Faculty of Engineering and Information Technology
at the University of Technology Sydney

by

Ngoc Thuy Le

Supervised by

Professor Doan B. Hoang

2019

Certificate of Original Authorship

I, Ngoc Thuy Le declare that this thesis, is submitted in fulfilment of the requirements for the award of the degree of Doctor of Philosophy, in the Faculty of Engineering and Information 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: Production Note: Signature removed prior to publication. Ngoc Thuy Le

Date: 18/12/2019

Dedication

To my parents and my parents in law

To my wife and daughter

To my brother

Thank you for your love and support

Acknowledgments

During the writing of this thesis, I have received a myriad of lessons, supports, and encouragements. First, I would like to express my deep gratitude to Professor Doan B. Hoang, my supervisor, for his enthusiastic encouragement, patient guidance, and precious lessons in keeping my PhD progress on schedule. He is one of my very important people as a mentor not only in teaching me the beauty of scientific research but also in guiding me in the way to balance between my family and my works. Perhaps, at the moments in my life, I will remember his words *"Please treat people with your love"* as an inspiration for me to dedicate myself to upholding the values of the society.

I would also like to extend my thanks to people who manage the UTS-VIED joint scholarship. I received this scholarship for my PhD course. This has been a wonderful opportunity to study in one of the best Universities in Australia. I wish to thank the School of Electrical and Data Engineering for providing me the funds for attending international conferences.

My special thanks to all my colleagues and friends embracing Dr. Priyadarsi Nanda, Dr. Zenon Chaczko, Tham Nguyen, Dat Dang, Chau Nguyen, Sara Farahmandian, Tuan Ha, Minh Pham, Ashish Nanda, and John Hazelton for their advice and assistance.

Finally, I would like to thank my parents, my parents in law, my wife and daughter, my brother and my sister in law for their encouragement and love over the four years. My wife and baby daughter always support and encourage me in my PhD course. They are always here for me. I wish to thank my parents for their wise counsel and sympathetic ears. This thesis is dedicated to them.

Sydney, December 2019.

The Author's Publications

International Conference Publications and Proceedings:

1 **Ngoc T. Le** and Doan B. Hoang. "Can maturity models support cyber security?" in *Performance Computing and Communications Conference (IPCCC), 2016 IEEE 35th International*, Las Vegas, USA, pp. 1-7. IEEE, 2016. (ERA Ranking: B)

2 **Ngoc T. Le** and Doan B. Hoang. "Threat probability computation using Markov and Common Vulnerability Scoring System" in *International Telecommunication Networks and Applications Conference (ITNAC), 2018 IEEE 28th International*, Sydney, Australia, 2018, pp. 1-7. (IEEE ITNAC); **Highly commended paper awards**. (ERA Ranking: B)

Journal papers:

3 **Ngoc T. Le** and Doan B. Hoang, "Capability Maturity Model and Metrics Framework for Cyber Cloud Security," *Scalable Computing: Practice and Experience* 18, no. 4 (2017): 277-290.

4 **Ngoc T. Le** and Doan B. Hoang, "A Threat Computation Model using a Markov Chain and Common Vulnerability Scoring System and its Application to Cloud Security", *Journal of Telecommunications and the Digital Economy*, vol. 7, no. 1, pp. 37-56, Mar. 2019.

5 **Ngoc T. Le** and Doan B. Hoang, "A new security threat model and computation the probability of Cloud security threats," submitted to *IEEE Transactions on Dependable and Secure Computing*. (Under Review)

6 **Ngoc T. Le** and Doan B. Hoang, "A Quantitative Security Metric for cloud security," submitted to *IEEE Transactions on Information Forensics and Security*. (Under Review)

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

APT	Advanced persistent threat
CIA	Confidentiality, Integrity, and Availability
CIS	Centre of Internet Security
CMM	Capability Maturity Model
CSA	Cloud Security Alliance
CSCMM	Cyber Security Capability Maturity Model
CVSS	The Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DOE	Department of Energy of the USA
DOS	Denial of Service
ENISA	European Union Agency for Network and Information Security
HTTPs	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a service
ICT	Information and Communication Technology
IDC	International Data Corporation
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OS	Operating System
OVF	Open Virtualisation Format
OWASP	The Open Web Application Security Project

PaaS	Platform as a service
QoS	Quality of Service
SaaS	Software as a service
SECaaS	Security as a service
SLA	Service Level Agreements
SQL	Structured Query Language
VPN	Virtual private network

Abstract

Cloud computing is a cutting-edge technology for building resource-sharing, on-demand infrastructures that support Internet of Things (IOTs), big data analytics, and software-defined systems/services. However, cloud infrastructures and their interconnections are increasingly exposed to attackers while accommodating a massive number of IOT devices and provisioning numerous sophisticated emerging applications.

There exist several cloud security models and standards dealing with emerging cloud security threats. They provide simplistic and brute-force approaches to addressing the cloud security problems: preventing security breaches by cautiously avoiding possible causes or fix them through trial and error attempts. Two major issues have been identified with the current approach to cloud security. First, it lacks quantitative measures in assessing the security level of security domains within a cloud space. Second, it lacks a model that can depict the overall security status of the cloud system.

In the light of the above, the aim of this dissertation is to investigate relevant quantitative security metrics and propose a novel Capability Maturity Model with Quantitative Security Metrics for Securing Cloud Computing. First, we propose a new security metric named Mean Security Remediation Cost to assess the cost attributed to cloud stakeholders when a security attack has occurred. Moreover, we propose three different quantitative novel models for quantifying the probability of a cloud threat materialising into an attack. Second, a new Cloud Security Capability Maturity Model (CSCMM) for the cloud will be proposed. The model includes cloud-specific security domains and the quantitative assessment of the overall security of the cloud under consideration. To support the measuring of security maturity levels, a security metric framework is introduced. The CSCMM Model will be quantitatively validated by proposed security metrics. We evaluate the model in a cloud computing environment and compare the consequences by simulating different parameters of the proposed security quantitative metric.

The thesis contributes to the theoretical body of knowledge in cloud security. The thesis proposes for the first time a Capability Maturity Model for cloud security. Additionally, the novel model will be used in practice by managers, security experts and

practitioners for both assessing the overall security status of the organisation/system and taking new quantitative measures to mitigate weaknesses of any specific aspects of the system as identified by the assessment. The major research outcomes from the thesis have been delivered in academic papers published in international peer-reviewed journals and conferences in cyber security and cloud computing.