A UNIFIED TRUST MODEL FOR COMMON CRITERIA RECOGNITION
ARRANGEMENT FOR PRODUCT ACCEPTANCE

MOHD ANUAR MAT ISA

FSKTM 2018 18
All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia
Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

A UNIFIED TRUST MODEL FOR COMMON CRITERIA RECOGNITION ARRANGEMENT FOR PRODUCT ACCEPTANCE

By

MOHD ANUAR MAT ISA

January 2018

Chair: Ramlan Mahmod, PhD
Faculty: Computer Science and Information Technology

Common Criteria (CC) is introduced as an international body for product testing, verification and certification. It is used for unifying existing international standards that involved users, vendors, manufacturers (industries) and governments. The purpose of the CC evaluation is to establish a one-time assessment without the need for a series of repetitive testing and verification processes for Common Criteria Recognition Arrangement (CCRA) participant nations. The trust problem arises between CC Authorizers and Consumers because the Consumers need to trust the Authorizer nation’s laboratory testing and verification of products. There are leading nations among the CCRA’s arrangement signatories (e.g. the USA) that want to reduce the mutual recognition level because the nations do not trust foreign nation’s laboratory testing and verification.

To overcome the trust problem, J. Kallberg proposed a hypothesis; which is to abandon the global approach of CCRA participants and replace it with well-established groups (e.g. EU, NATO). Secondly, the thesis has improved the J. Kallberg suggestion by introducing intersection members (nations) among the well-established groups that can serve as bridges to spread trust boundaries. A nation that a member of more than one group has a wider coverage of transitive trust. Then, the nation will act as a bridging nation between different groups. Thirdly, in order to minimize the trust gap between CCRA participant nations, choosing a nation that has good international relations with many nations as a candidate for the authorizing nation. This will minimize the trust problem if one chooses a nation that is good international relations as the authorizing nation compared to a nation has historical controversy which may lead to doubtful perception.

In this work, the thesis has modeled and verified the proposed solutions in minimizing the trust problem using a process of relation algebra and formal methods. Precedent methods such as Bayes probability, Dempster-Shaffer theory and subjective logic are referred to. The modeling steps as follows,
selecting requirements and formal specifications; implement and verify the models using Event-B and Atelier theorem prover. The verified models were simulated using ProB simulator for finding trustable CC authorizing nations using case studies from the period 1999 until 2014.

The performance measurement of the proposed models was evaluated based on trust relations of the CC authorizing nations with other CCRA nations; and the trust relations metrics were displayed as a list of CC authorizing nations ranking. From the simulation results, the ranking has shown that the USA, NLD, ESP, ITA, FRA and DEU dominated as the trustable authorizing nations. The thesis has suggested that the CCRA participant nations should choose the authorizing nation with the highest ranking because it is more trustable compared to lower ranking authorizing nations. As the conclusion, choosing the highest ranking authorizing nation can minimize the trust problem between the CCRA participant nations.
Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Doktor Falsafah

MODEL KEPERCAYAAN BERSEPADU UNTUK PIAWAIAN PRODUK ANTARABANGSA DENGAN MENGGUNAKAN PENGIKTIRAFAN KRITERIA BERSAMA

Oleh

MOHD ANUAR MAT ISA

Januari 2018

Pengerusi: Ramlan Mahmod, PhD
Fakulti: Sains Komputer dan Teknologi Maklumat

Kriteria Umum (CC) diperkenalkan sebagai piawaian antarabangsa untuk ujian, pengesahan dan pensijilan produk. Ia digunakan untuk menyatukan piawaian antarabangsa sedia ada yang melibatkan pengguna, penjual, pengeluar (industri) dan kerajaan. Tujuan penilaian CC adalah untuk menubuhkan penilaian sekali tanpa memerlukan beberapa siri proses pengujian dan pengesahan berulang untuk Negara Peserta Pengiktirafan Pengiktirafan Kriteria (CCRA). Masalah ketidak kepercayaan timbul antara pengesah dan pegguna CC kerana pengguna perlu mempercayai pengujian dan pengesahan produk makmal negara pemeriksa. Terdapat negara terkemuka yang telah menandatangan perjanjian CCRA (misalnya Amerika Syarikat) yang ingin mengurangkan tahap pengiktirafan bersama kerana kurang mempercayai ujian makmal dan pengesahan negara asing.

Untuk mengatasi masalah amanah, J. Kallberg mencadangkan suatu hipotesis yang mencadangkan untuk meninggalkan pendekatan global Peserta CCRA dan menggantikannya dengan kumpulan antarabangsa yang stabil (cth. EU, NATO). Kedua, tesis telah meningkatkan cadangan J. Kallberg dengan memperkenalkan ahli-ahli persilangan (negara-negara) di kalangan kumpulan antarabangsa yang stabil yang boleh berfungsi sebagai jambatan untuk menyebaran kepercayaan kepada kumpulan yang berlainan. Negara yang menyertai lebih dari satu kumpulan mempunyai liputan kepercayaan yang lebih luas. Negara ini akan bertindak sebagai negara penghubung antara kumpulan yang berlainan. Ketiga, untuk mengurangkan jurang ketidak kepercayaan antara negara-negara peserta CCRA, tesis telah mencadangkan untuk memilih negara yang mempunyai hubungan internasional yang baik dengan banyak negara lain sebagai calon negara pengesah. Ini akan mengurangkan masalah ketidak kepercayaan jika memilih negara yang mempunyai hubungan antarabangsa yang baik sebagai negara yang diberi pengesah berbanding negara yang mempunyai kontroversi sejarah yang mungkin membawa kepada persepsi keraguan.

Pengukuran prestasi model yang dicadangkan dinilai berdasarkan hubungan kepercayaan dari negara-negara yang pesesah CC; dan metrik perhubungan kepercayaan dipaparkan sebagai senarai pesesah CC. Dari hasil simulasi, senarai pesesah telah menunjukkan bahawa USA, NLD, ESP, ITA, FRA dan DEU sebagai negara yang pesesah yang boleh dipercayai. Negara peserta CCRA harus memilih negara pesesah yang mempunyai kedudukan tertinggi di dalam senarai pesesah kerana ia lebih dapat dipercayai berbanding dengan negara-negara pesesah yang berada di senarai terbawah. Sebagai kesimpulan, memilih negara pesesah yang berada di kedudukan tinggi dapat mengurangkan masalah ketidak percayaan antara negara peserta CCRA dengan menggunakan penyelesaian yang telah dicadangkan.
ACKNOWLEDGEMENTS

I wish to convey my heartfelt gratitude to Professor Dr. Ramlan Mahmod, Associate Professor Dr. Nur Izura Udzir, Dr. Ali Dehghantanha and Dr. Jamalul-lail Ab Manan for their help on my journey to complete this research work as well as the thesis. Without them, I could not have ever imagined that this day would ever happen.

I would like to express my thanks to my family and friends for their support during the journey. I also want to acknowledge the Ministry of Education (MOE) Malaysia for providing MyBrain15 (MyPhD) scholarship and Universiti Putra Malaysia (UPM) for supporting the research work. Thank you.
I certify that a Thesis Examination Committee has met on 16 January 2018 to conduct the final examination of Mohd Anuar Mat Isa on his thesis entitled “A Unified Trust Model for Common Criteria Recognition Arrangement for Product Acceptance” in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the degree of Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

**Md Nasir Sulaiman, PhD**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

**Zuriati Ahmad Zukarnain, PhD**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
/Internal Examiner

**Azizol Abdullah, PhD**
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
/Internal Examiner

**Abdullah Mohd Zin, PhD**
Professor
Faculty of Computer Science and Information Technology
Universiti Kebangsaan Malaysia
Malaysia
/External Examiner

[Nor Aini AB. SHUKOR, PhD]
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 27 February 2018
This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

**Ramlan Mahmod, PhD**  
Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Chairman)

**Nur Izura Udzir, PhD**  
Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

**Ali Dehghantanha, PhD**  
Senior Lecturer  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

**Jamalul-Iail Ab Manan, PhD**  
Director  
Information Security Department  
MIMOS Berhad  
(Member)

---

**ROBIAH BINTI YUNUS, PhD**  
Professor and Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date:
Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: __________________________ Date: ____________

Name and Matric No.: Mohd Anuar Bin Mat Isa (GS31348)
Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: Name of Chairman of Supervisory Committee:

Ramlan Mahmud

Signature: Name of Member of Supervisory Committee:

Nur Izura Udzir

Signature: Name of Chairman of Supervisory Committee:

Ali Dehghantanha

Signature: Name of Member of Supervisory Committee:

Jamalul-lail Ab Manan
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>i</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>v</td>
</tr>
<tr>
<td>APPROVAL</td>
<td>vi</td>
</tr>
<tr>
<td>DECLARATION</td>
<td>viii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xiii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xv</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>xvi</td>
</tr>
</tbody>
</table>

## CHAPTER

### 1 INTRODUCTION

1.1 Overview                                    1
1.2 Problem Statement                           2
1.3 Hypothesis                                  3
1.4 Research Objective                          3
1.5 Research Scope                              4
1.6 Research Contributions                      4
1.7 Thesis Organization                         5

### 2 LITERATURE REVIEW

2.1 Introduction                                7
2.2 International Information Security Standards 7
  2.2.1 Trusted Computer System Evaluation Criteria (TCSEC) 7
  2.2.2 Information Technology Security Evaluation Criteria (ITSEC) 8
  2.2.3 Common Criteria (CC)                          8
2.3 Trust Definition                            12
2.4 Trust Calculus                               13
  2.4.1 Bayesian Theory                             14
  2.4.2 Dempster-Shafer Theory                      14
  2.4.3 Subjective Logic (Algebra)                  15
2.5 Event-B                                     17
2.6 Related Literature                          19
  2.6.1 Trust Definition                           19
  2.6.2 Trust Formalism                            19
  2.6.3 International Relations Methodology         20
  2.6.4 Trust on Recommendation (Reputation) System 20
  2.6.5 Trust on International Relations            21
  2.6.6 Formal Verification and Simulation          24
  2.6.7 Common Criteria                            25
  2.6.8 Common Criteria and Formal Verification     26
2.7 Literature Analysis and Discussion           27
2.8 Summary                                     32
3 METHODOLOGY
3.1 Introduction 33
3.2 Methodology Overview 33
3.3 Formulation of Research Hypothesis 38
3.4 Identification of Case Studies 39
  3.4.1 International Relations 39
  3.4.2 CCRA Participant and International Groups 40
  3.4.3 Generic CCRA workflows 41
3.5 Design and Implementation of Trust Models 41
  3.5.1 RAIR 41
  3.5.2 NGTM, GCM and CTM 42
3.6 Model Verification 42
  3.6.1 Formal Verification 42
  3.6.2 Model Simulation using Case Studies 43
3.7 Performance Measurement 44
3.8 Summary 45

4 TRUST MODEL
4.1 Introduction 46
4.2 Mapping Between Trust Problem and Trust Model 46
4.3 Relation Algebra for International Relations (RAIR) 48
  4.3.1 Definition and Notation 48
  4.3.2 Design and Implementation 53
  4.3.3 Relation Algebra and Computation 54
4.4 Formal Methods: NGTM, GCM and CTM 60
  4.4.1 Modeling and Notation in Event-B 61
  4.4.2 Proving Method 64
4.5 Generic CCRA Model (GCM) 66
4.6 Nation in Group Trust Model (NGTM) 69
4.7 CCRA Trust Model (CTM) 71
4.8 Summary 75

5 FORMAL VERIFICATION
5.1 Introduction 76
5.2 Generic CCRA Model (GCM) 76
  5.2.1 Model Requirement 76
  5.2.2 Formal Specification 78
  5.2.3 Model and Refinement 79
  5.2.4 Model Verification 87
5.3 NGTM 89
  5.3.1 Model Requirement 89
  5.3.2 Formal Specification 91
  5.3.3 Model and Refinement 92
  5.3.4 Model Verification 97
5.4 CTM 100
  5.4.1 Merge Model and Refinement 101
  5.4.2 Model Verification 103
5.5 Summary 105
## 6 SIMULATION RESULTS AND DISCUSSION

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Introduction</td>
<td>106</td>
</tr>
<tr>
<td>6.2</td>
<td>Experimental Design</td>
<td>106</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Experiment Setup</td>
<td>106</td>
</tr>
<tr>
<td>6.2.2</td>
<td>Data Requirements</td>
<td>108</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Performance Measurement</td>
<td>108</td>
</tr>
<tr>
<td>6.3</td>
<td>Relation Algebra for International Relations (RAIR)</td>
<td>109</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Results</td>
<td>109</td>
</tr>
<tr>
<td>6.3.2</td>
<td>Discussion</td>
<td>117</td>
</tr>
<tr>
<td>6.4</td>
<td>Generic CCRA Model (GCM)</td>
<td>119</td>
</tr>
<tr>
<td>6.4.1</td>
<td>Results</td>
<td>119</td>
</tr>
<tr>
<td>6.4.2</td>
<td>Discussion</td>
<td>120</td>
</tr>
<tr>
<td>6.5</td>
<td>Nation in Group Trust Model (NGTM)</td>
<td>122</td>
</tr>
<tr>
<td>6.5.1</td>
<td>Results</td>
<td>122</td>
</tr>
<tr>
<td>6.5.2</td>
<td>Discussion</td>
<td>125</td>
</tr>
<tr>
<td>6.6</td>
<td>CCRA Trust Model (CTM)</td>
<td>127</td>
</tr>
<tr>
<td>6.6.1</td>
<td>Results</td>
<td>127</td>
</tr>
<tr>
<td>6.6.2</td>
<td>Discussion</td>
<td>132</td>
</tr>
<tr>
<td>6.7</td>
<td>Hypothesis Testing</td>
<td>136</td>
</tr>
<tr>
<td>6.8</td>
<td>Model Testing</td>
<td>137</td>
</tr>
<tr>
<td>6.8.1</td>
<td>Model Consistency by Same Datasets</td>
<td>137</td>
</tr>
<tr>
<td>6.8.2</td>
<td>Model Consistency by Spin-off Datasets</td>
<td>137</td>
</tr>
<tr>
<td>6.9</td>
<td>Result Comparison</td>
<td>146</td>
</tr>
<tr>
<td>6.10</td>
<td>Summary</td>
<td>150</td>
</tr>
</tbody>
</table>

## 7 CONCLUSION

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Introduction</td>
<td>151</td>
</tr>
<tr>
<td>7.2</td>
<td>Summary</td>
<td>151</td>
</tr>
<tr>
<td>7.3</td>
<td>Research Challenges</td>
<td>151</td>
</tr>
<tr>
<td>7.4</td>
<td>Research Contributions</td>
<td>154</td>
</tr>
<tr>
<td>7.5</td>
<td>Future Work</td>
<td>155</td>
</tr>
<tr>
<td>7.6</td>
<td>Closing Remark</td>
<td>156</td>
</tr>
</tbody>
</table>

### REFERENCES

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>156</td>
</tr>
</tbody>
</table>

### APPENDICES

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>168</td>
</tr>
</tbody>
</table>

### BIODATA OF STUDENT

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>205</td>
</tr>
</tbody>
</table>

### LIST OF PUBLICATIONS

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>206</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>CC evaluation concepts</td>
</tr>
<tr>
<td>2.2</td>
<td>An overview of general work flows in CC</td>
</tr>
<tr>
<td>2.3</td>
<td>Binomial opinions using trangle diagram</td>
</tr>
<tr>
<td>2.4</td>
<td>Verification stages for Event-B</td>
</tr>
<tr>
<td>2.5</td>
<td>Cognitive map of V.V. Putin’s trust perceptions by Y. Lutsenko</td>
</tr>
<tr>
<td>3.1</td>
<td>An overview of CC trust models with input-output data flows</td>
</tr>
<tr>
<td>3.2</td>
<td>CTM process flows</td>
</tr>
<tr>
<td>3.3</td>
<td>GCM process flows</td>
</tr>
<tr>
<td>3.4</td>
<td>NGTM process flows</td>
</tr>
<tr>
<td>3.5</td>
<td>RAIR process flows</td>
</tr>
<tr>
<td>3.6</td>
<td>Diagram describing iterative nature of the hypothetico-deductive method</td>
</tr>
<tr>
<td>4.1</td>
<td>The mapping between trust problem and trust model</td>
</tr>
<tr>
<td>4.2</td>
<td>A summary of relation algebra for international relations</td>
</tr>
<tr>
<td>4.3</td>
<td>An overview of implementation of NGTM, GCM and CTM using Event-B in Rodin platform</td>
</tr>
<tr>
<td>4.4</td>
<td>Add_Authorizer event in M2_CC_Model</td>
</tr>
<tr>
<td>4.5</td>
<td>Detail rules for Add_Authorizer/inv1/INV and its conclusion sequents</td>
</tr>
<tr>
<td>4.6</td>
<td>A list of roles in context C2_CC_Model</td>
</tr>
<tr>
<td>4.7</td>
<td>A simulation of M3_CC_Model_Analysis model</td>
</tr>
<tr>
<td>4.8</td>
<td>A list of nations in the context of the C1_CC_Model</td>
</tr>
<tr>
<td>4.9</td>
<td>A list of international groups in context C3_CC_Model</td>
</tr>
<tr>
<td>4.10</td>
<td>A simulation of M6_Trust_Model_Analysis model</td>
</tr>
<tr>
<td>4.11</td>
<td>A simulation of M7_CC_Trust_Model_Analysis model</td>
</tr>
<tr>
<td>4.12</td>
<td>List_Authorizer_In_Group event</td>
</tr>
<tr>
<td>4.13</td>
<td>List_of_Authorizers_In_Overlapped_Group event</td>
</tr>
<tr>
<td>4.14</td>
<td>List&gt;All_Authorizer event</td>
</tr>
<tr>
<td>5.1</td>
<td>GCM’s machines and contexts</td>
</tr>
<tr>
<td>5.2</td>
<td>C1 context</td>
</tr>
<tr>
<td>5.3</td>
<td>C2 context</td>
</tr>
<tr>
<td>5.4</td>
<td>M1 invariants and variables</td>
</tr>
<tr>
<td>5.5</td>
<td>M2 invariants and variables</td>
</tr>
<tr>
<td>5.6</td>
<td>M3 List Authorizer event</td>
</tr>
<tr>
<td>5.7</td>
<td>M3 List Consumer event</td>
</tr>
<tr>
<td>5.8</td>
<td>Discharged Proof Obligations for M1, M2 and M3</td>
</tr>
<tr>
<td>5.9</td>
<td>M3 simulation</td>
</tr>
<tr>
<td>5.10</td>
<td>Counter_Authorizer_Level event</td>
</tr>
<tr>
<td>5.11</td>
<td>NGTM’s machines and contexts</td>
</tr>
<tr>
<td>5.12</td>
<td>C3 context</td>
</tr>
<tr>
<td>5.13</td>
<td>M4’s invariants and variables</td>
</tr>
<tr>
<td>5.14</td>
<td>M5’s invariants and variables</td>
</tr>
<tr>
<td>5.15</td>
<td>Discharged Proof Obligations for M4, M5 and M6</td>
</tr>
<tr>
<td>5.16</td>
<td>M6 simulation</td>
</tr>
<tr>
<td>5.17</td>
<td>Nation_Overlapped_Grouping_And_Relation_Score event</td>
</tr>
<tr>
<td>5.18</td>
<td>CTM’s machines and contexts</td>
</tr>
</tbody>
</table>
5.19 Discharged Proof Obligations for M7
5.20 M7 simulation
5.21 List_All_CC_Authorizer events
6.1 Data for Relation Properties in MySQL database.
6.2 A summary of relations neutral, friendly and hostile for the 34 nations
6.3 A statistics of CC’s certified products
6.4 Selected states with unsorted results in List_Authorizer_In_Group event
6.5 Selected states with unsorted results in List_Authorizer_In_Overlapped_Group event
6.6 A total ranking using four events in M7 simulation
6.7 A total ranking using three events in M7 simulation
6.8 GCM shows original model states before Canada is removed from Authorizer role.
6.9 GCM shows Remove_Authorizer event being selected for a process to remove Canada’s role from Authorizer
6.10 GCM shows variance outcomes for Counter_Authorizer_Level event when Canada’s role as Authorizer was removed
6.11 NGTM shows original model states before the Great Britain is removed from EU group
6.12 NGTM shows Disjoin_Group event being selected for a process to remove the Great Britain from EU as a spin-off dataset
6.13 NGTM shows variance outcomes for Nation_Overlapped_Grouping_And_Relation_Score event when the Great Britain was removed from EU as a spin-off dataset
6.14 CTM shows original model states before Malaysia is removed from Authorizer role.
6.15 CTM shows Remove_Authorizer event being selected for a process to remove Malaysia’s role from Authorizer
6.16 CTM shows variance outcomes for List_Authorizer_In_Overlapped_Group event when Malaysia’s role as Authorizer was removed
6.17 A snapshot of content analysis results from Y. Lutsenko’s thesis
LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>An example of relation between two nations</td>
</tr>
<tr>
<td>2.2</td>
<td>The summary of precedent related works</td>
</tr>
<tr>
<td>4.1</td>
<td>A list of Properties</td>
</tr>
<tr>
<td>4.2</td>
<td>Properties of the USA and GBR</td>
</tr>
<tr>
<td>4.3</td>
<td>Properties of the USA and IRN</td>
</tr>
<tr>
<td>4.4</td>
<td>Properties of the USA and IND</td>
</tr>
<tr>
<td>4.5</td>
<td>Set-theoretical notation</td>
</tr>
<tr>
<td>4.6</td>
<td>List of predicates</td>
</tr>
<tr>
<td>4.7</td>
<td>Usage of predicates</td>
</tr>
<tr>
<td>5.1</td>
<td>Model requirements for GCM</td>
</tr>
<tr>
<td>5.2</td>
<td>Formal specifications for GCM</td>
</tr>
<tr>
<td>5.3</td>
<td>Summary for all events in GCM</td>
</tr>
<tr>
<td>5.4</td>
<td>Model requirements for NGTM</td>
</tr>
<tr>
<td>5.5</td>
<td>Formal specifications for NGTM</td>
</tr>
<tr>
<td>5.6</td>
<td>Summary for all events in NGTM</td>
</tr>
<tr>
<td>5.7</td>
<td>Summary for all events in CTM</td>
</tr>
<tr>
<td>6.1</td>
<td>A summary of the relation algebra for the International Relations case study</td>
</tr>
<tr>
<td>6.2</td>
<td>A summary of EALs</td>
</tr>
<tr>
<td>6.3</td>
<td>A summary of Roles</td>
</tr>
<tr>
<td>6.4</td>
<td>A result of List_All_Relation event</td>
</tr>
<tr>
<td>6.5</td>
<td>A result of Group_Relationship_Score event</td>
</tr>
<tr>
<td>6.6</td>
<td>A result of Nation_Overlapped_Grouping_And_Relation_Score event</td>
</tr>
<tr>
<td>6.7</td>
<td>A ranking from List_Authorizer_In_Group event</td>
</tr>
<tr>
<td>6.8</td>
<td>A ranking from List_Authorizer_In_Overlapped_Group event</td>
</tr>
<tr>
<td>6.9</td>
<td>A ranking from List_All_Authorizer event</td>
</tr>
<tr>
<td>6.10</td>
<td>A ranking from List_All_CC_Authorizer event</td>
</tr>
<tr>
<td>6.11</td>
<td>Total of all rankings (or a trust metric for Authorizers)</td>
</tr>
<tr>
<td>6.12</td>
<td>RAIR shows variance outcomes for Israel when property P6 was set to false</td>
</tr>
<tr>
<td>6.13</td>
<td>Total of all Ranking have changed after Malaysia become formerl Authorizer</td>
</tr>
<tr>
<td>6.14</td>
<td>The summary of comparison between the previous works and thesis results</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria</td>
</tr>
<tr>
<td>AU</td>
<td>African Union</td>
</tr>
<tr>
<td>AI</td>
<td>artificial intelligent</td>
</tr>
<tr>
<td>CPNIG</td>
<td>CCRA Participant Nations and International Groups</td>
</tr>
<tr>
<td>CTM</td>
<td>CCRA Trust Model</td>
</tr>
<tr>
<td>CCRA</td>
<td>Common Criteria Recognition Arrangement</td>
</tr>
<tr>
<td>CIA</td>
<td>confidentiality, integrity and availability</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DRM</td>
<td>digital right management</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level</td>
</tr>
<tr>
<td>GCM</td>
<td>Generic CCRA Model</td>
</tr>
<tr>
<td>GWOT</td>
<td>Global War on Terrorism</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITSEC</td>
<td>Information Technology Security Evaluation Criteria</td>
</tr>
<tr>
<td>ICBM</td>
<td>intercontinental ballistic missile</td>
</tr>
<tr>
<td>INV</td>
<td>invariant</td>
</tr>
<tr>
<td>MNNA</td>
<td>Major non-NATO ally</td>
</tr>
<tr>
<td>NGTM</td>
<td>Nation in Group Trust Model</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NAM</td>
<td>Non-Aligned Movement</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>OIC</td>
<td>Organisation of Islamic Cooperation</td>
</tr>
<tr>
<td>PF</td>
<td>probability function</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profile</td>
</tr>
<tr>
<td>RAIR</td>
<td>Relation Algebra for International Relations</td>
</tr>
<tr>
<td>SARs</td>
<td>Security Assurance Requirements</td>
</tr>
<tr>
<td>SFRs</td>
<td>Security Functional Requirement</td>
</tr>
<tr>
<td>ST</td>
<td>Security Target</td>
</tr>
<tr>
<td>TCSEC</td>
<td>Trusted Computer System Evaluation Criteria</td>
</tr>
<tr>
<td>TCB</td>
<td>Trusted Computing Base</td>
</tr>
<tr>
<td>TOE</td>
<td>Target of Evaluation</td>
</tr>
<tr>
<td>UNASUR</td>
<td>Union of South American Nations</td>
</tr>
<tr>
<td>UN</td>
<td>United Nation</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Overview

International standards and certifications play a major role in product distributions and marketing activities. To be well accepted in the global market, all IT products and services require international evaluations and certifications such as the Common Criteria (CC) certification. CC is an international standard body utilized for certifying security products and services. The CC is used for information technology security evaluation that covers features such as: generic security model; security functions; and security assurance components. The standard is published in order to unify the pre-existing security standard for users, vendors, manufacturers (industries) and governments in utilizing standard security requirements and evaluations.

There are six key features in CC [1]–[3]: Target of Evaluation (TOE), Protection Profile (PP), Security Target (ST), Security Functional Requirements (SFRs), Security Assurance Requirements (SARs), and Evaluation Assurance Level (EAL) respectively. TOE is a product or system for CC evaluation. PP is security requirements that should be imposed to the TOE. Manufacturer or vendor must comply their product with PP(s). ST is a standard document that identifies various security properties for TOE evaluation. It may consist one or more PPs. SFRs are security functions that are individually provided by a product. SARs are descriptions of testing that were done to a product. It shows how the product meets a security compliant or security claims. EAL is a rating of a product after passed security evaluations (or SARs). The rating begins with one (EAL1) as a basic security assurance, and seven (EAL7) is the most rigorous security assurance and most expensive one.

By the CCRA agreement, all signatories (participants) have agreed to recognize EALs one until four [1] except the United State of America is EALs one until two [2], [4]. Through EALs recognition scheme, all CCRA Consumers agree to recognize CCRA Authorizer’s evaluations [1], [5], which it may be done by a foreign Authorizer [6]. The goal of the CC mutual recognition is “to eliminate the burden of duplicating evaluations of IT products and protection profiles” as well as “to improve the efficiency and cost-effectiveness of the evaluation” [1], [5]. At the last quarter 2016, there are 17 Authorizers and 10 Consumers in CCRA. The CCRA mutual recognition requires its signatories to trust foreign nation security assessments for IT products, which may introduce an unofficial refusal to consume a certified product [6]. For example, restless international relations between Authorizer (e.g. Turkey) and Consumer (e.g. Israel) nations may lead to this problem [6].
1.2 Problem Statement

Recent literature studies [2], [4], [6] have mentioned that the CC paradigm is exposed to the issue of a trust problem in a mutual recognition of CC certification among CCRA participant nations. The trust problem will render the usage of CC as the international body responsible for international certification. The problem is affected by an issue of trust in regard to international relations and foreign policy of nations. The CC paradigm is vulnerable to this issue when the trust problem arises between the CCRA participant nations. This major problem was addressed by J. Kallberg (2012) [6] in his manuscript entitled “Common Criteria meets Realpolitik - Trust, Alliances, and Potential Betrayal”. He argues that a mutual recognition of CC among nations that are not the closest of allies makes national policymakers unwilling to accept it even though they have signed CCRA. Kallberg's argument is grounded on a national security policy whereby when a national security is at stake, a country tends to become more selfish and concentrate on protecting its own interests. Therefore, if the country policy maker has a lessen trust to the CC Authorizer, then it will render the trustworthiness of the certified product by the CC Authorizer. The trust problems addressed by Kallberg were supported by Kurth (2012) [4] and Ragen (2013) [2]. Both have mentioned that there are leading nations among the CCRA's arrangement signatories (e.g. the USA) that want to reduce the mutual recognition level to lower than Evaluation Assurance Level (EAL) 2 (including augmentation).

The trust problem arises between CC Authorizer and Consumer because the Consumer needs to trust the Authorizer nation’s laboratory testing and verification of products [6]. This mutual recognition can, in theory, result in a reduction of cost, resources, and time, but may change due to any complication that may arise in the areas of international relations, foreign policy and national security policy. The trust problem between Authorizer to Consumer has not been well addressed as yet, and there is no direct solution for minimizing the trust problem between Authorizer and Consumer. Referring to the trust problem addressed by Kallberg [6], Kurth [4] and Ragen [2], the thesis has divided the problem statement into three sub-problems as follows:

i. To address the trust problem between nations that have signed CCRA for product acceptance [2], [4], [6]. The international relations between CCRA participant nations should be identified which either friendly (allies), neutral, or hostile. The trust exists between nations that are the closest ally or friendly (e.g. the USA and UK) compared to nations that have historically confrontation (e.g. the USA and Soviet Union/Russia) [6]. Therefore, the international relations between the CCRA participant nations must be identified before one can choose the trustable Authorizer.

ii. To address the trust problem within the international groups which have CCRA participant nations as its members [6], namely NATO; EU; OIC; NAM; and MNNA. The trust literatures [6]–[13] have shown that nations establish and join international groups because of mutual benefits from a coalition (alliance). Coalition nations in the international groups believe that the coalition participants will honor the international coalition with a certain degree of trust. Therefore, finding trustable nations as Authorizer in the
international groups may help to minimize the trust problem between Authorizer and Consumer [6].

iii. To address the trust problem within Common Criteria (CC), the CC should be modeled for identifying CCRA’s workflow [14] and the respective roles of CCRA participant nations [1]. The roles can be either Consumer, Authorizer or Manufacturer. Based on the given roles, the Authorizer can be identified for trust evaluation metrics using trust in international relations and trust in international groups.

1.3 Hypothesis

This section presents a research hypothesis (or proposed solution) for the thesis. Based on the problem statement, we use it as a prediction for a tentative conclusion (or research outcome) of this research work [6], [15]. The thesis hypothesis is defined as:

“Trust in international relations exists between Authorizers and Consumers of CCRA participant nations, and the finest authorizer can be determined from among Authorizers that are friendly and neutral towards many of the CCRA participant nations.”

The finest or trustable Authorizer is ideally a nation which has the highest of trust relations with other CCRA participant nations. Simulation of CCRA Trust Model (CTM) with case studies will provide an output of a trust metric (relation) for all Authorizers. The trust metric is calculated using a “group of trust” theory as suggested by J. Kallberg [6]; an overlapping of the “group of trust”; and international relations of all Authorizers with CCRA participant nations. Based on these three categories (variables), the four models, and collected data as case studies, we want to show that the trust problem between Authorizer and Consumer nations can be minimized by choosing the finest Authorizer. It will allow a higher chance of mutual recognition and acceptance of the CC certification among the CCRA participant nations. Consequently, it will help lessen potential vulnerability of the CC paradigm when a trust problem arises between the CCRA participant nations. A deduction of the thesis’s hypothesis will be discussed at the end of Chapter 6.

1.4 Research Objective

The objective of this study is to propose a unified trust model for CC, which is then used to determine the trustable authorizing nation in CCRA. The outcome of the research goal is to minimize the trust problem between Authorizer and Consumer nations. In order to achieve the objective, the following processes will be carried out:

i. To design a mathematical formalism for “classifying international relations” between CCRA participant nations. This will allow international relations computation between CCRA participant nations as well as to find the trustable Authorizer.
ii. To design a formal model for international groups which have CCRA participant nations as its members. This will help identify mutual interests and trust relations of CCRA participant nations in the international groups. The trustable Authorizer by international group classification will be identified.

iii. To design a formal model for CCRA’s workflow and the respective roles of CCRA nations. The Authorizer can be identified for trust evaluation using the CCRA’s workflow and the respective roles using modeling technique. This will also help convey a foreground in understanding the CC evaluation processes to all CC stakeholders.

1.5 Research Scope

This work only used public data which available on the Internet as sources for international relations between CCRA participant nations. An observation by the authors for data collections was done for a limited duration, which will be discussed in Chapter 3. We focused on the headlines trust issues in international relations as inputs for the study. The last chapter provides a brief justification on why we chose to use the public data (including headlines news) on the Internet as the inputs.

1.6 Research Contributions

The research contributions of the thesis are as follows:

i. **A unified trust model for CC**: We present the unified CCRA Trust Model (CTM) to determine the finest authorizing member in CCRA. The CTM combines RAIR, NGTM and GCM models.

ii. **A method by which to compute international relations**: This is a formal calculus of Relation Algebra for International Relations (RAIR) designed for international relations computation. The proposed method will allow international relations computation, which has previously been subjective and incomputable. The method will help to provide government decision-makers (e.g. foreign ministry, defense ministry or presidential) with strategic information concerning other nations.

iii. **A formalism of international relations of nations in an international group**: This is a formal model of Nation in Group Trust Model (NGTM) for international group modeling. None of the existing literature has ever modeled international groups and its member relations. The NGTM will help to identify mutual interests and trust relations of its members such as: defense alliances; economic cooperation agreements; politics and foreign policy; historical events etc.

iv. **A formalism of CC workflows**: This is a formal model of Generic CCRA Model (GCM) designed for the CCRA workflow. Prior literature has
discussed a formalism of product security using CC methodology [16]–[27] but, to date, nobody has ever modeled and verified the CC workflow and its architecture as stated in the CCRA document [1]. The GCM can help convey a foreground in understanding the CC evaluation processes to all stakeholders including: evaluators; evaluation sponsors; system developers; consumers and vendors [14]. This modeling work focuses on relationships between Authorizer, Consumer and Manufacturer (or vendor) in CC’s value chain.

v. **A trust metric for all CCRA authorizer nations**: Based on the data collected from case studies, we explored the entire material concerning CCRA participant nations and its relations. We have mapped the trust metric for 17 Authorizers as a trust ranking for all Authorizers. We used ProB simulator to simulate the finest authorizing nation using CTM. A timeline for the case studies covered the period from 1999 until 2014 (15 years). We gathered public data for all case studies over a 6 months period (July 2014 to December 2014). One may use the trust ranking in order to choose the most suitable Authorizer for a product security testing and verification process.

1.7 **Thesis Organization**

Chapter 1: Introduction.
This chapter provides an overview of the entire research work undertaken for this thesis. It discusses research problems, hypothesis, objectives and contributions respectively.

Chapter 2: Literature Review.
This chapter revisits the state of the art research works. It discusses issues such as: information security standards (e.g. CC); trust definition and its calculus; formal methods; international relations; and related multidiscipline literature.

Chapter 3: Methodology.
This chapter explains the research methodology applied for this research work. It details a formulation of the research hypothesis, identification of case studies, design and implementation of all models, as well as a model verification and simulation using formal methods.

Chapter 4: Trust Model.
This chapter presents the design and implementation of the proposed trust model. It discusses the four models, namely: RAIR, NGTM, GCM and CTM.

Chapter 5: Formal Verification.
This chapter presents model verifications for NGTM, GCM and CTM using formal methods. The model verification is divided into four stages, specifically: model requirement; formal specification; model design and refinement; and model verification.
Chapter 6: Simulation Result and Discussion.  
This chapter displays simulation results of the four models. The four models are tested using actual data from the case studies. Simulation results for all models are discussed here. The truth of the thesis’s hypothesis is also verified here.

Chapter 7: Conclusion.  
This chapter wraps up the thesis achievements with regard to its goals, objectives and research contributions. Lastly, we have suggested some future work whereby the findings made in this study can be extended.
REFERENCES


[35] Porta, P. L. and Scanzieri, R., "Towards an economic theory of international civil society: Trust, trade and open government", *Structural


Lutsenko, Y., "Trust in International Relations: Case-Study of Russian-Finnish Cooperation", University of Tampere, 2011.

J. Wheeler, N., "Trust-Building in International Relations", *Peace Prints*:


Lecomte, T., "Safe and reliable metro platform screen doors control/command systems", FM 2008: Formal Methods, Lecture Notes in


[187] "Embassy of Switzerland -Foreign Interests Section", 2015. [Online].
Available: https://www.eda.admin.ch/countries/iran/en/home/representations/emba-
ssey-of-switzerland-foreign-interests-section.html. [Accessed: 17-Nov-
2015].

Nov-2015].
17-Nov-2015].
Available: http://www.pbs.org/wgbh/pages/frontline/showdown/themes/grandbargai-
[192] "Public Statement on U.S. Policy Toward the Iran Nuclear Negotiations", 
analysis/view/public-statement-on-u.s.-policy-toward-the-iran-nuclear-
[Online]. Available: http://www.business-
standard.com/article/specials/clinton-imposes-full-sanctions-on-india-
[195] Dan Balz and William Drozdiak, "U.S. Responds With Penalties,
http://www.washingtonpost.com/wp-
srv/inatl/longterm/southasia/stories/penalties051498.htm. [Accessed: 18-
Nov-2015].
[196] Council on Foreign Relations, "Agreement for Cooperation Between the 
Government of the United States of America and the Government of India 
Concerning Peaceful Uses of Nuclear Energy (123 Agreement)", 2007. 
[Online]. Available: http://www.cfr.org/india/agreement-
cooperation-between-government-united-states-america-government-india-
concerning-peaceful-uses-nuclear-energy-123-agreement/p15459. 
[197] Esther Pan, J. B., "The U.S.-India Nuclear Deal", Council on Foreign 
2015].
[200] Burghardt, G. M. et al., "Perspectives - Minimizing Observer Bias in 
[201] Delbufalo, E., "Subjective trust and perceived risk influences on 
exchange performance in supplier-manufacturer relationships",


