ISSN 1 746-7233, England, UK
World Journal of Modelling and Simulation
Vol. 13 (2017) No. 3, pp. 173-182

A formal verification and simulation of common criteria recognition arrangement (CCRA)*

Mohd Anuar Mat Isa[1†] and Ramlan Mahmod[1] and Nur Izura Udzir[1] and Jamalul-lail Ab Manan[1] and Ali Dehghantanha[2] and Solahuddin Shamsuddin[3]

[1] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia
[2] University of Salford, The Crescent, Salford, United Kingdom
[3] CyberSecurity Malaysia, Selangor, Malaysia

(*Received June 05 2016, Accepted May 04 2017*)

Abstract. Common Criteria (CC) is an international standard body for certifying security products and services. CC is used for information technology security evaluation that covers generic security model, security functional and security assurance components. The standard is published to unify pre-existing security standard for users, vendors, manufactures (industries) and government in using standard security requirements and evaluations. This publication is the first attempt in an information security research that is to CCRA model and simulates it. The purpose of this research work is to help CC's stakeholders to further understand CC's framework using a modeling and simulation. The CCRA model will deliver a generic model of CC relationships between a product manufacturer, product authorizer and product consumer in the CC's supply chains. We use Event-B as modeling language (notation), Atelier-B as theorem prover and ProB as a simulation tool. We also provide a case study for a simulation.

Keywords: common criteria, ccra, formal methods, simulation, verification, international standard

1 Introduction

This publication describes an extension of the authors previous works[16, 17, 27] that related to trust issues in CC. Prior to that in 1983, US Department of Defense (DoD) saw the significance of globalization and they began emphasizing many defense strategies to protect US interest in the world[22]. DoD wanted to position as world leader in information security and defense technologies, then introduced Multi-Level Security (MLS), which was documented in a series of book publications called Rainbow Series. The main book was always being referenced in computer security area is Trusted Computer System Evaluation Criteria (TCSEC) and also known as Orange Book[30]. The Orange Book had been becoming a foundation for Information Technology Security Evaluation Criteria (ITSEC) that was released in 1990. After that, CC standard is introduced based on a mutual agreement between World War II countries such as USA, UK, France and Germany. This agreement uses to standardize the evaluation of security in IT technologies and related products [26]. This work attempts to model CC framework for evaluation and certification of IT products. It will help CC stakeholders to understand the CC framework using a modeling technique by formal methods.

The authors research work began in 2012, which emphasize the need for a "trust model" in CC. It stressed on trust as an important element to ensure CCRA participating nations to mutually recognizes and consume CC products. Previous work motivation is influenced by J. Kallberg suggestion that "the long-term survival of CC requires abandoning the global approach and instead use established groupings of trust"[19]. The research

* The authors would like to acknowledge the Ministry of Higher Education (MOHE) Malaysia for providing research funding, and Universiti Putra Malaysia (UPM) for supporting this research work.
† Corresponding author. *E-mail address*: anuarls@hotmail.com

objectives of this work are 1) to model a generic framework of CCRA model and to verify it using formal methods; and 2) to simulate the proposed CCRA model using existing CCRA's data sets (as a case study).

The outline of this publication is as follows. Literature reviews on preceding works in Related Work section. It follows by Methodology section that summarizes research methodology used in modeling CCRA. Then modeling stages of the CCRA in Model Design and Implementation section. CCRA verification using CCRA's data sets as a case study in Model Testing section. Results and discussion of the case study simulation with regard to CC's statistics in Discussion section. Future works planning, which related in expanding the CCRA model in Future Work section. Summarization of this research contribution in Contribution section. Lastly, closing remarks in Conclusion section.

2 Related work

2.1 International information security standards

This section presents three international information security standards: Trusted Computer System Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC) and Common Criteria (CC). TCSEC and ITSEC were the prior art of CC. TCSEC (or named Orange Book) established by the United State Government in Department of Defense (DoD) under National Security Agency (NSA). It was introduced in 1985, and it had been used to evaluate computer systems and its resources[30]. It was used to evaluate security criteria by 4 classes with priority and classified level. ITSEC was introduced to address requirements of security protection in Information Technology (IT) systems or products. ITSEC documentations were first published in European countries in 1990 and succeeding its publication in 1991 by Commission of European Communities. European countries had used ITSEC to evaluate IT based related products and services. The main requirements for evaluation are confidentiality, integrity and availability (CIA), and it was referred to as assurance for security systems or products[26].

CC is introduced for information technology security evaluation that covers generic security model, security functional and security assurance components. It was initiated in 1998, by a group of countries, namely Canada, United Kingdom, France and Germany, which have signed CCRA to recognize CC evaluations for IT security products. CC is used to unify pre-existing security standard for users, vendors, manufacturers (industries) and government for standard security requirements and evaluations. The security evaluation can help to establish a level of confidence for a security functionality of IT products. An assurance measurement (evaluation criteria) is applied to test against IT products and its results may help consumers to conclude whether they meet the accepted standard of security requirements or fail to meet what they claimed[24, 25].

2.2 Formal methods

Formal methods or formal calculus is a mathematical technique for a model verification. The model verification can be divided into a few stages such as a requirement, specification, architectural design and detail design[2]. The purpose formal verification is to establish mathematical analysis that contributes to reliability, safety (or failsafe) and robustness of software or hardware designs[3]. Refer to Fig. 1, formal methods is applied to various stages in product development. The formal verifications process can be done using proving tools such as theorem prover, model checking or abstract interpretation[6, 14].

2.3 Modeling using event-B

Event-B[3] is a mathematical modeling tool for a modeling, analysis and verification of systems. It uses a set theory as a core language and notation. Event-B introduces by Jean-Raymond Abrial (inventor of notations B) as an expansion of B notation. Event-B is integrated into Rodin platform[3, 11] using IDE Java Eclipse and plugins. Event-B uses Atelier B plugin[21] as a third-party theorem prover for a model verification process. In this work, all proof obligations are discharged using default installed prover NewPP in Rodin and third-party provers from the Atelier B: provers PP and ML[3, 18]. ProB is also integrated into the Rodin platform[13]

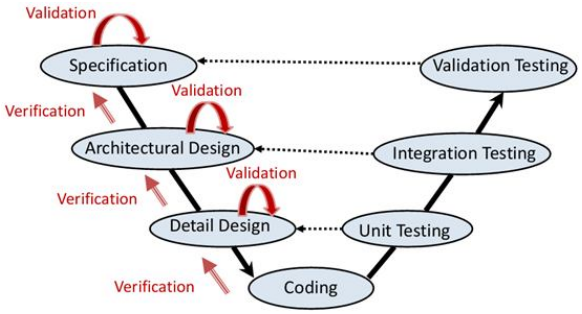


Fig. 1: Verification stages for Event-B[2]

as a plugin for a model animation and model checking. The ProB helps in a model debugging using model simulation.

Event-B consists of a collection of state variables and guards that are used to control state variables[3]. Event-B modeling work can be divided into two parts: context and machine. The context (e.g. Fig. 3) is used for defining constants and axioms of a model e.g. constant is NATION and e.g. axiom is Finite (NATION). These are static parts of Event-B. The machine is used for defining model variables or states and it is a dynamic part of Event-B. We need to manipulate the dynamic part as major efforts in designing and verifying a formal model. Variables (or states) can be a constant for basic mathematical objects such as sets and its elements, relations, functions and sequence of numbers. These constants will be used in arithmetic operation on certain data types in Event-B. To control and manipulate the arithmetic operation, the constants must be guarded using invariants . The invariants must be checked and proved, and it must hold (true) for every modification in the states.

An event will trigger a change(s) in variable(s) and it must not violate an invariant(s). To guarantee the invariant always holds, the event must be controlled using a guard and an action. The guard will provide conditions similar to "if statement" and the action will give condition resemble to "then statement" in a programming language. The guard will check necessary conditions for the event to be triggered. The action will change a value of variable(s) or state(s) in a model after the event triggered. One need to be cautious in designing a model because the guard(s) and the action(s) will cause a violation to the invariant(s). To introduce a new model from the old one, machine refinement is used. It is called a concrete machine for the old model, and an abstract machine for a new refined machine. Machine refinement will provide model improvements from the previous one by adding, removing or expanding events, guards, invariants etc.

2.4 Related literature review

There are quite a number of past works that related to formal methods and CC modeling. (Abrial and Mussat[5] introduce dynamic constraints that allow a model to evolve using B notation. Motr and Tri[28] provided a case study of a smart card verification using B method. The author used CC methodology to verify the smart card. Prieto-Diaz[29] provides a complete report regarding CC evaluation process. The purpose of the report is to bring a foreground in the understanding of CC evaluation process to all stakeholders such as an evaluator, sponsors, system developer, consumers and vendors. Watson and Wildman[36] verified a Trusted Filter device for CC security testing using Event-B. Ware et al.[35] facilitate a method to handle security requirements using CC methodology. Mellado et al.[23] discussed reusable aspects of security requirements in CC. Yamamoto et al.[38] proposed a security case study based on CC security structure and analysis. Kaneko et al.[34] introduce a method to describe security assurance in CC evaluation process that is suitable for an analysis of security and threat.

Abrial and Hallerstede[4] present crucial methods for modeling large and complex systems using a refinement, decomposition and instantiation in Event-B. Wright[37] developed an automatic source codes generator in C language for Event-B's model. Bendisposto and Leuschel[6] add a ProB plugin in Rodin platform that supports a model checking for Event-B. Hallerstede et al.[33] provide a multilevel of animation in ProB that is

used to simulate a model with a multilevel refinement of machines. Iliasov[15] improve Event-B specification using a visualization and diagram. Kaur et al.[20] compare three major formal methods notations that in term of formal specification languages: Z, B and VDM. Métayer et al [1, 7, 10] report on development and verification of a complex system using mathematical modeling technique (e.g. Event-B). Rezazadeh et al.[31] redesigned a formalism of Commercial Air Traffic (CAD) Information System (CDIS) and results showed that those weaknesses can be solved using Event-B refinements. Yeganefard et al.[32] provided a systematic way to model a control problem in Event-B.

We had reviewed related works: CC, formal methods and modeling. From observations in the literatures, we found no one has worked on CCRA model. The nearest work by [29] that is to bring a mutual understanding of the CC evaluation process to all stakeholders. Based on the literature reviews, we have selected Event-B as a modeling language for this research work. The Event-B can be considered as a mature modeling language, and it is an industry practical used [12] for formal verification. In the literature reviews, one can observe that there are many publications mentioned the practice of Event-B in CC for product evaluations (e.g. EALs) and formalisms of product evaluation processes. Another reason for the Event-B because it is integrated into Rodin platform. ProB and Atelier B help a lot in debugging for finding invariance violations in the model, and it can make our job faster to discharge proof obligations. Furthermore, a proved model can be easily simulated using ProB simulator. It allows a user to input datasets (or case study's data), and then it can produce results as tabular (refer to Fig. 4). The ProB simulator demonstrates pleasant interactions during model simulation (e.g. it shows the entire model's states and a very interactive of model's events). It can aid user to perform a model demonstration to third-parties (stakeholders) such as sponsors and customers. They can see the entire model's states and state transitions (e.g. variable value) that can be done by clicking at GUI of the ProB simulator.

3 Methodology

We began by the construction of a research hypothesis. We derived the research hypothesis by performing literature reviews that related to modeling CCRA using formal methods. During the literature reviews phase, we have identified case study for the CCRA model. Based on the case study and CCRA documents[8], we selected some of requirements that require implementing a generic CCRA model. Based on the selected requirements, we transform it into formal specifications. Then, we simplified the formal specifications by combining or removing insignificant requirements. The insignificant requirements can be categorized as real world interactions and it is not practical to be modeled. The formal specifications transformed into a formal model using Event-B notations. Then, the formal model verified using a built-in Rodin's prover and Atelier B prover for discharging proof obligations. The verified model tested using a ProB simulator. We divided simulation works using ProB into two parts: first, testing with random data and animations; and second, testing with existing CCRA's datasets. The results of the simulations are presented in Fig. 4 and Tab. 1, and it can be compared to the CC's statistics[9]. The Methodology section serves as a guideline of this research work.

4 Model design and implementation

4.1 Ccra model

Fig. 2 shows an overview of CCRA. We derived it from CCRA document[8]. In this work, we do not model the entire requirements from the CCRA document. We have selected some of the requirements that are necessary to implement the CCRA model. It must tie to the research objectives as aforementioned.

4.2 Refinement strategy

Fig. 3 shows Event-B refinement strategy for CCRA model. It consists of three machines: an initial model M1, first refinement of model M2, and second refinement of model M3; and two contexts: a first context C1 and second context C2. The C1 defines a finite element of sets NATION and PRODUCT. The C2 defines a

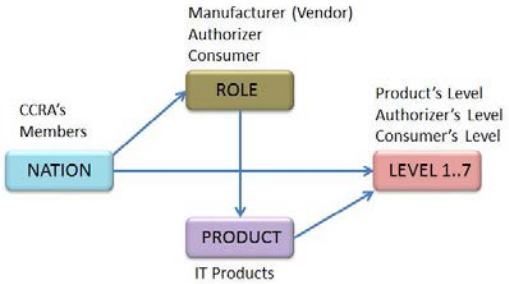


Fig. 2: An overview of CCRA model

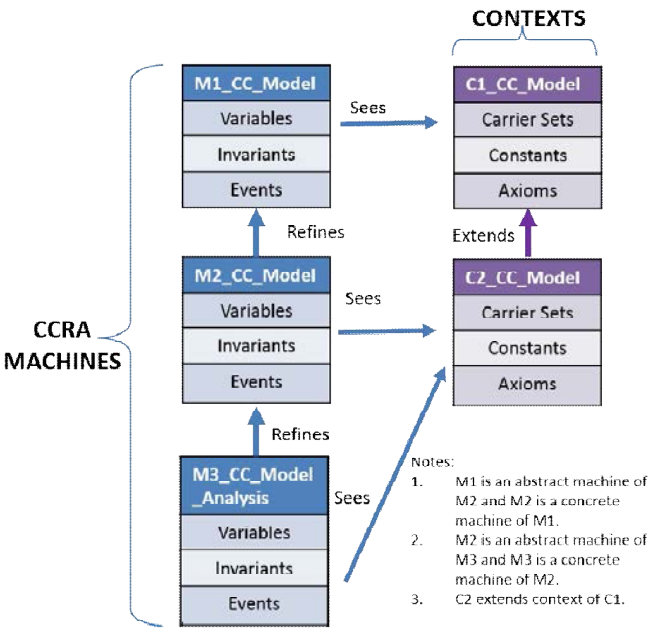


Fig. 3: Machine refinements and context extensions for CCRA model

finite element of set ROLE and a finite constant LEVEL with elements between 1 until 7. The ROLE represents that either a nation can be Manufacturer, Authorizer or Consumer. The constant LEVEL represents CCRA's compliance in Evaluation Assurance Levels (EAL) from 1 to 7. M3 does not change anything (not refine) from the first refined model M2. It uses for the model analysis in the simulation phase using plugin ProB. We should not use the M3 for a next model refinement, but one should use the M2 for the next model refinement. The second model refinement (M3) does not provide an additional improvement for the first model refinement (M2). This refinement is used to observing CCRA model's states in term of relations, partial functions, invariances and etc. We have used the M3 as statistic queries for displaying the CCRA model's states.

5 Model testing: the CCRA case study

In this section, NATION set is represented by CCRA's members and non-CCRA's members. We have divided a case study into four parts: five-year timelines in 2000, 2005, 2010 and 2015. To simplify the model testing, we chose to use existing data concerning CCRA's Authorizers and CCRA's Consumers. We had avoided the actual elements for PRODUCT set because of CC have certified too many products. For an instance, certified CC's products are almost two thousand by the end of the year 2015[9]. To model the actual number of certified products will consume a huge amount of computing power (e.g. memory to store and compute input sequents, proof rules etc.) and it will be very difficult to discharge too many proof obligations (prover timeout will occur).

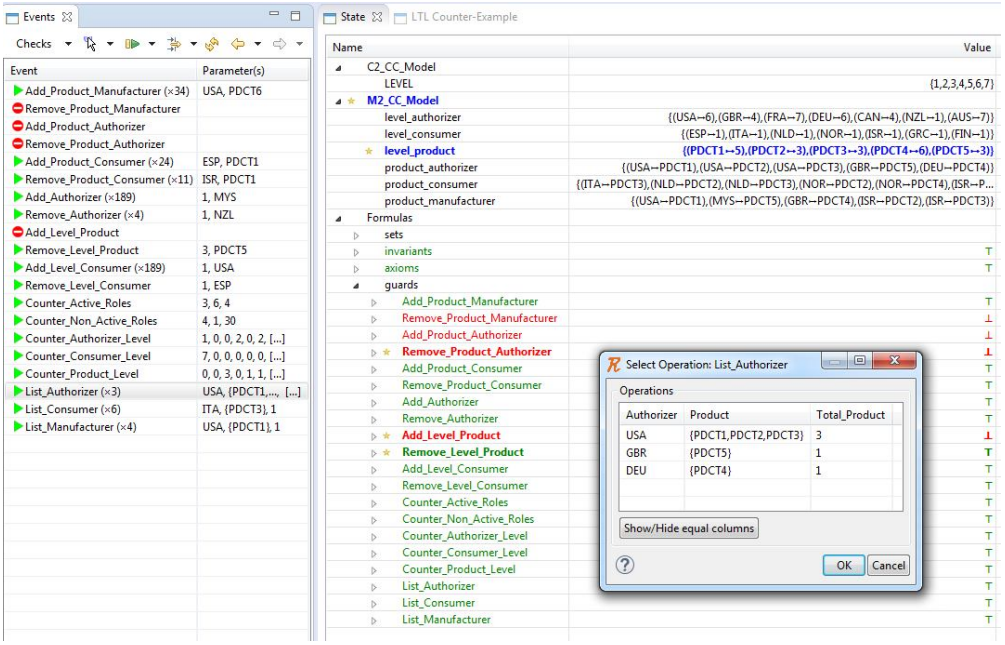


Fig. 4: M3_CC_Model_Analysis using CCRA's participant in the year 2000 (with random data)

To test events used PRODUCT, we added some random products that will ensure the events to be triggered in ProB simulation. These random products are added in the year 2000 timeline as presented in Fig. 4.

CCRA participant nations simulation is categorized into four timelines: 2000, 2005, 2010 and 2015 without random data. We have assumed that each CCRA's consumer will accept a lowest certified product level, EAL1. Tab. 1 shows results the four categories without: the random data, random states in variables relation and partial function. The Tab. 1 shows only results for variables level_authorizer and level_consumer. Observe in the Tab. 1, we highlighted columns "TOTAL" and "SUM BOTH" because both columns are not in CCRA model. It can help a reader to grasp a total calculation. Furthermore, an event Counter_Active_Roles is zero because we do not trigger any event related to PRODUCT. The Counter_Active_Roles previously simulates using random data as presented Figure 4. We also did not trigger an event that can cause an authorizer nation become a consumer for an authorized product. This is practically happening in CC and CCRA model is also work for a requirement such that "when a nation become an authorizer in CCRA arrangement, the nation is also turn out to be a consumer". For an example, we can add an authorizer nation to be a consumer with consumer's EAL. It is a bit tricky if we show it in the table because each nation can be a manufacturer, consumer and authorizer. In this modeling work, we add 34 nations, but only 26 nations are CCRA's signatories.

6 Discussion

This paragraph will discuss the existing products certified by CC. Fig. 5 shows statistics of CC's certified products. From the Fig. 5, there is a plus sign after a word "EAL$< 1 \cdots 7 >$", indicating that there is an augmentation(s) of security requirements for a given evaluated product. In this modeling work, we have omitted the product augmentations because we want to simplify modeling complexity. We can observe that there are almost 2000 products passed the EAL by the end of the year 2015. By these number of certified products, it is not practical to include the actual number of the certified products in PRODUCT set for this modeling work.

Furthermore, CC's statistics did not list any nation that is currently a consumer to the certified CC's products. We do not want to argue a trust issue in this work, but we want to show that CCRA can be modeled and verified with sufficient efforts. In this modeling work, we do not include a maximum level of EAL mutual recognition (this should be in a future work), but each consumer can choose their minimal acceptance level of EAL. By a default value in this model, a consumer will accept EAL1 as showed in Tab. 1. A fascinating part in

this work, we want to perform ProB simulation such that it will show CCRA model's states that can be similar to CC's statistics in Fig. 5. It can be done using a model refinement for a model analysis, which is alike to Fig. 4.

Table 1: A summary of the variables level_authorizer and level_consumer using the M3_CC_Model_Analysis for timelines 2000, 2005, 2010 and 2015.

	Evaluation Assurance Level (EAL):	L1	L2	L3	L4	L5	L6	L7	TOTAL	SUM BOTH
2000	Counter_Authorizer_Level	1	0	0	2	0	2	2	7	14
	Counter_Consumer_Level	7	0	0	0	0	0	0	7	
2005	Counter_Authorizer_Level	1	0	0	3	0	2	2	8	23
	Counter_Consumer_Level	15	0	0	0	0	0	0	15	
2010	Counter_Authorizer_Level	1	0	0	5	4	2	3	15	26
	Counter_Consumer_Level	11	0	0	0	0	0	0	11	
2015	Counter_Authorizer_Level	1	0	0	7	4	2	3	17	26
	Counter_Consumer_Level	9	0	0	0	0	0	0	9	
		CC_Authorizer			CC_Consumer				CC_Manufacturer	
2000	Counter_Active_Roles	0			0				0	
	Counter_Non_Active_Roles	7			7				34	
2005	Counter_Active_Roles	0			0				0	
	Counter_Non_Active_Roles	8			15				34	
2010	Counter_Active_Roles	0			0				0	
	Counter_Non_Active_Roles	15			11				34	
2015	Counter_Active_Roles	0			0				0	
	Counter_Non_Active_Roles	17			9				34	

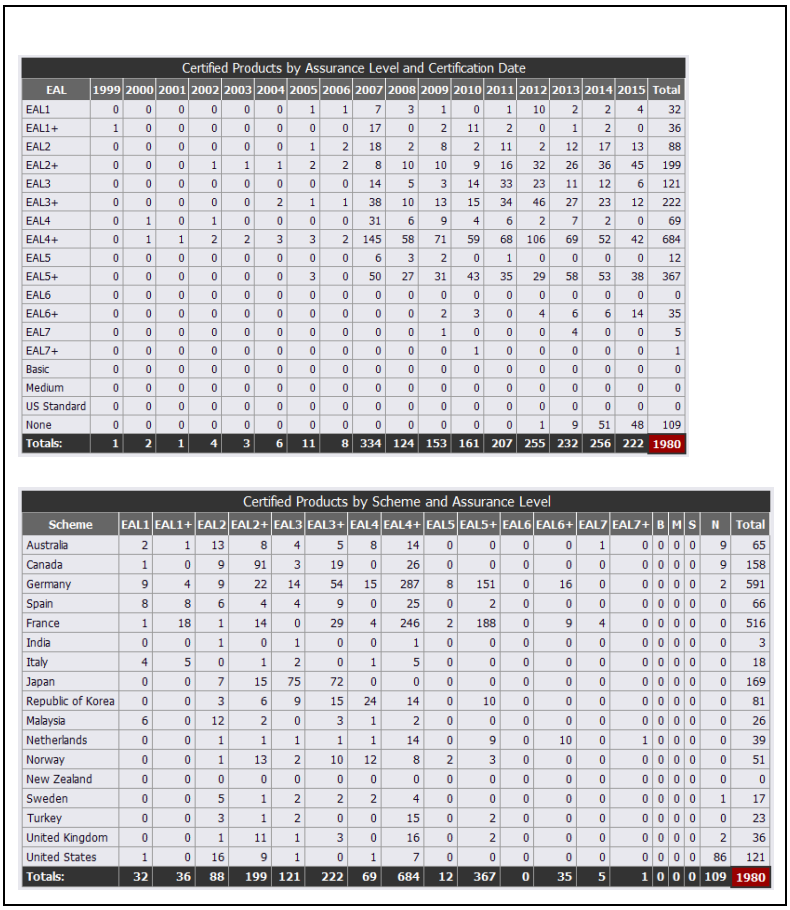
7 Future work

We are planning to improve CCRA model by adding trust elements in a future CCRA model. It requires additional refinement of machine and context, invariants, events and etc. For comprehensive model analysis, more local variables in events will be added. The purpose of a trust model for the CCRA is to evaluate trust based on international relations between CCRA participant nations.

8 Contribution

CCRA model has incorporated some of requirements in CCRA document. We have implemented nation roles, EAL's product, level of authorizer in a product evaluation, and level of consumer in consuming certified CC's products. Based on the selected requirements, we tested it in ProB simulator. The CCRA model can be used to simulate actual data using M3_CC_Model_Analysis, which it also can be used to query model's states during simulation. For examples, local variables (in events) can be displayed as columns and the model's states can be displayed as rows in ProB GUI (refer to Fig. 4). The M3_CC_Model_Analysis can be implemented and simulated as a query system, which is to perform an access to CC database. The results of the M3_CC_Model_Analysis can be customized as statistics of CCRA's Management Information Systems (MIS). Later, CCRA model can be used to provision CC's statistics as showed in Fig. 5.

Refer to literature reviews in the Related Work section, we have done exhaustive searches for an implementation of CCRA using a modeling technique (by means formal methods) and we have found nothing. From the literature reviews, there were many literatures discussed a formalism of product evaluation process for a Common Methodology for Information Technology Security Evaluation (CEM) [24]. CC's accreditation authorities use the CEM documentations as an evaluation methodology (or guidelines) to evaluate security of products. Some literatures discussed modeling works using model checking to verify the CEM with a Target of Evaluation (TOE). We believed that, we have done the first attempt in an information security research to



Certified Products by Assurance Level and Certification Date

EAL	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
EAL1	0	0	0	0	0	0	1	1	7	3	1	0	1	10	2	2	4	32
EAL1+	1	0	0	0	0	0	0	0	17	0	2	11	2	0	1	2	0	36
EAL2	0	0	0	0	0	0	1	2	18	2	8	2	11	2	12	17	13	88
EAL2+	0	0	0	1	1	1	2	2	8	10	10	9	16	32	26	36	45	199
EAL3	0	0	0	0	0	0	0	0	14	5	3	14	33	23	11	12	6	121
EAL3+	0	0	0	0	0	2	1	1	38	10	13	15	34	46	27	23	12	222
EAL4	0	1	0	1	0	0	0	0	31	6	9	4	6	2	7	2	0	69
EAL4+	0	1	1	2	2	3	3	2	145	58	71	59	68	106	69	52	42	684
EAL5	0	0	0	0	0	0	0	0	6	3	2	0	1	0	0	0	0	12
EAL5+	0	0	0	0	0	0	3	0	50	27	31	43	35	29	58	53	38	367
EAL6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL6+	0	0	0	0	0	0	0	0	0	0	2	3	0	4	6	6	14	35
EAL7	0	0	0	0	0	0	0	0	0	0	1	0	0	0	4	0	0	5
EAL7+	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
Basic	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	0	0	0	0	0	1	9	51	48	109
Totals:	**1**	**2**	**1**	**4**	**3**	**6**	**11**	**8**	**334**	**124**	**153**	**161**	**207**	**255**	**232**	**256**	**222**	**1980**

Certified Products by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia	2	1	13	8	4	5	8	14	0	0	0	0	1	0	0	0	0	9	65
Canada	1	0	9	91	3	19	0	26	0	0	0	0	0	0	0	0	0	9	158
Germany	9	4	9	22	14	54	15	287	8	151	0	16	0	0	0	0	0	2	591
Spain	8	8	6	4	4	9	0	25	0	2	0	0	0	0	0	0	0	0	66
France	1	18	1	14	0	29	4	246	2	188	0	9	4	0	0	0	0	0	516
India	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	3
Italy	4	5	0	1	2	0	1	5	0	0	0	0	0	0	0	0	0	0	18
Japan	0	0	7	15	75	72	0	0	0	0	0	0	0	0	0	0	0	0	169
Republic of Korea	0	0	3	6	9	15	24	14	0	10	0	0	0	0	0	0	0	0	81
Malaysia	6	0	12	2	0	3	1	2	0	0	0	0	0	0	0	0	0	0	26
Netherlands	0	0	1	1	1	1	1	14	0	9	0	10	0	1	0	0	0	0	39
Norway	0	0	1	13	2	10	12	8	2	3	0	0	0	0	0	0	0	0	51
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	0	0	5	1	2	2	2	4	0	0	0	0	0	0	0	0	0	1	17
Turkey	0	0	3	1	2	0	0	15	0	2	0	0	0	0	0	0	0	0	23
United Kingdom	0	0	1	11	1	3	0	16	0	2	0	0	0	0	0	0	0	2	36
United States	1	0	16	9	1	0	1	7	0	0	0	0	0	0	0	0	0	86	121
Totals:	**32**	**36**	**88**	**199**	**121**	**222**	**69**	**684**	**12**	**367**	**0**	**35**	**5**	**1**	**0**	**0**	**0**	**109**	**1980**

Fig. 5: Statistics of CC's certified products on 04 Nov 2015 (Common Criteria, 2015)

model the CCRA. The CCRA model can deliver value chains of the entire architecture of CC. Based on the information we have up to now, the existing research works used CC's methodology or paradigm to verify IT products security using formal methods for EALs 5 until 7; but no one has verified the CC itself using formal methods. This is the first attempt, we believed that it is a novel work to model the CC or CCRA. We also acknowledge that, our CCRA model is not complete yet. There are many research gaps and opportunities, which it is still open for future research works.

9 Conclusion

In this work, we model a workflow of CCRA using Event-B. This publication intention is to model some of CCRA's requirements. We have met the research objectives by implementing and verifying CCRA model using formal methods. The outcome of this research work is a generic model of CCRA. We have also tested the CCRA model using random data and CCRA's data sets (case study) in ProB simulator. The ProB simulator showed an interactive simulation process and well-organized results (e.g. data or simulation results presented as tabular). The results of the model simulation can be used by CC's stakeholders as a method for CC analysis and decision making. The CCRA model is not the final outcome from this research work and we are expecting a future work to be delivered as soon as possible.

References

[1] F. K. S. A. Kusagur, R. Sanker. Modelling & simulation of an anfis controller for an ac drive. *World Journal of Modelling and Simulation*, 2012, **8**(1): 36–49.

[2] J. R. Abrial. *Modeling in Event-B: System and Software Engineering*. Cambridge University Press, 2010.
[3] J. R. Abrial, M. Butler, S. Hallerstede, T. S. Hoang, F. Mehta, L. Voisin. Rodin: an open toolset for modelling and reasoning in event-b. *International Journal on Software Tools for Technology Transfer*, 2010, **12**(6): 447–466.
[4] J. R. Abrial, S. Hallerstede. Refinement, decomposition, and instantiation of discrete models: Application to event-b. **in:** *International Workshop on Abstract State Machines, Asm 2005, March 8-11, 2005, Paris, France*, 2007, 17–40.
[5] J. R. Abrial, L. Mussat. Introducing dynamic constraints in b. **in:** *International B Conference on Recent Advances in the Development and Use of the B Method*, 1998, 83–128.
[6] J. Bendisposto, M. Leuschel. Proof assisted model checking for b. *Lecture Notes in Computer Science*, 2009, **5885**: 504–520.
[7] J.-R. A. C. Mtayer, L. Voisin. Rigorous open development environment for complex systems, 2005. Project IST-511599 RODIN.
[8] C. Criteria. Arrangement on the recognition of common criteria certificates in the field of it security, 2014.
[9] C. Criteria. Certified products list - statistics, 2015.
[10] P. J. Durst, C. Goodin. High fidelity modelling and simulation of inertial sensors commonly used by autonomous mobile robots. *World Journal of Modelling and Simulation*, 2012, **8**(3): 172–184.
[11] Event-b.org. Event-b and the rodin platform, 2014.
[12] J. Fitzgerald, J. Bicarregui, P. G. Larsen, J. Woodcock. *Industrial Deployment of Formal Methods: Trends and Challenges*. Springer Berlin Heidelberg, 2013.
[13] S. Hallerstede, M. Leuschel, D. Plagge. *Validation of formal models by refinement animation*. Elsevier North-Holland, Inc., 2013.
[14] C. Heitmeyer, M. Archer, E. e. a. Leonard. Applying formal methods to a certifiably secure software system. *IEEE Transactions on Software Engineering*, 2008, **34**(1): 82–98.
[15] A. Iliasov. Use case scenarios as verification conditions: event-b/flow approach. **in:** *International Conference on Software Engineering for Resilient Systems*, 2011, 9–23.
[16] M. A. M. Isa, R. Mahmod, N. I. e. a. Udzir. A formal calculus for international relations computation and evaluation. 2016.
[17] M. A. M. Isa, J. A. Manan, R. e. a. Mahmod. Game theory: Trust model for common criteria certifications & evaluations. *International Journal of Cyber-Security and Digital Forensics*, 2012, **1**(1).
[18] M. Jastram, P. M. Butler. *Rodin User's Handbook*. CreateSpace Independent Publishing Platform, 2015.
[19] J. Kallberg. The common criteria meets realpolitik: Trust, alliances, and potential betrayal. *IEEE Security & Privacy*, 2012, **10**(4): 50–53.
[20] A. Kaur, G. M. Samridhi, M. S. Singh. Analysis of three formal methods-z, b and vdm. **in:** *International Journal of Engineering Research and Technology*.
[21] T. Lecomte. *Atelier B*. John Wiley & Sons, Inc., 2014.
[22] D. Mackenzie, G. Pottinger. Mathematics, technology, and trust: Formal verification, computer security, and the u.s. military. *IEEE Annals of the History of Computing*, 1997, **19**(3): 41–59.
[23] D. Mellado, E. Fernndez-Medina, M. Piattini. A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces*, 2007, **29**(2): 244–253.
[24] C. C. Members. Common criteria for information technology security evaluation part 1: Introduction and general model july 2009 revision 3 final, 2009.
[25] C. C. Members. Common criteria for information technology security evaluation, 2011.
[26] I. Members. Information technology security evaluation criteria (itsec), 1991.
[27] R. M. Mohd Anuar Mat Isa, Jamalul-lail Ab Manan, et al. Finest authorizing member of common criteria certification. **in:** *CyberWarfare and Digital Forensic 2012* (J. P. Xu, ed.), CyberWarfare and Digital Forensic 2012, 2012, 166–171.
[28] S. Motr, C. Tri. Using b method to formalize the java card runtime security policy for a common criteria evaluation. 2000, 1–16.
[29] R. Prieto-Diaz. The common criteria evaluation process, process explanation, shortcomings, and research opportunities. 2002.
[30] L. Qiu, Y. Zhang, F. e. a. Wang. Trusted computer system evaluation criteria. *Classified Information*, 1985.
[31] A. Rezazadeh, N. Evans, M. Butler. Redevelopment of an industrial case study using event-b and rodin. **in:** *Th Internatioanal Conference on Formal Methods in Industry*, 2007, 6–6.
[32] M. B. S. Yeganefard, A. Rezazadeh. Evaluation of a guideline by formal modelling of cruise control system in event-b, 2010. Eprints.ecs.soton.ac.uk.
[33] H. Stefan, L. Michael, P. Daniel. *Refinement-Animation for Event-B ł Towards a Method of Validation*. Springer Berlin Heidelberg, 2010.
[34] Y. Wang. Conference article title. **in:** *The International Conference on Computer Security and Digital Investigation (ComSec2014)* (J. P. Xu, ed.), 2005, 29–35.

[35] M. S. Ware, J. B. Bowles, C. M. Eastman. Using the common criteria to elicit security requirements with use cases. **in:** *SoutheastCon, 2006. Proceedings of the IEEE*, 2006, 273–278.

[36] G. Watson, L. Wildman. *Common Criteria Compliance for the Trusted Filter at EAL7-Formal Arguments*. Technical Report, 2008.

[37] S. Wright. Automatic generation of c from event-b. **in:** *SoICT '11 Proceedings of the Second Symposium on Information and Communication Technology*, 2009.

[38] S. Yamamoto, T. Kaneko, H. Tanaka. *A Proposal on Security Case Based on Common Criteria*. Springer Berlin Heidelberg, 2013.