Game Theory: Trust Model for Common Criteria Certifications & Evaluations

Mohd Anuar Mat Isa[1], Jamalul-lail Ab Manan[2], Ramlan Mahmod[3],
Habibah Hashim[4], Nur Izura Udzir[5], Ali Dehghan Tanha[6], Mar Yah Said[7]

Faculty of Computer Science &
Information Technology, 43400 UPM
Serdang, Selangor, Malaysia.
[1]anuarls@hotmail.com
[3]ramlan@fsktm.upm.edu.my
[5]izura@fsktm.upm.edu.my
[6]alid@fsktm.upm.edu.my
[7]maryah@fsktm.upm.edu.my

Advanced Analysis and Modeling Cluster,
MIMOS Berhad, Technology Park
Malaysia,
57000 Kuala Lumpur, Malaysia.
[2]jamalul.lail@mimos.my

Faculty of Electrical Engineering,
40450 UiTM Shah Alam,
Selangor, Malaysia.
[4]habib350@salam.uitm.edu.my

Abstract— International standard and certification play major role in product distributions and marketing activities. To be well accepted in global market, all IT products and services require international evaluation and certification such as Common Criteria (CC) certification. This paper discusses some of the security, trust and privacy issues in Common Criteria that would happen during evaluation and certification of IT products and services. Our main intention is to help interested stake holders in choosing a finest authorizing member of CC certification for IT products and services using our new trust model. The proposed trust models takes into account the dynamically changing international relationship among nations which produces an index value during selection of finest CC authorizing member. The trust models use game theory to identify the finest CC authorizing member. We hope to contribute to this area of research by lessening the "cost to market" of IT products and related services. It is anticipated that it would give positive impact on global business transaction by having better and wider acceptability using our models in the selection of the finest CC authorizing member, CC consumer, and vendor (manufacturer).

Keywords – Common Criteria, Game Theory, CC, TCSEC, ITSEC, Coorperative Game, Non Coorperative Game, Minmax, Zero-sum game, Nash Equilibrium, Dominance Strategy, Dominant Strategy, Security, Evaluation, Assessment, Privacy, Trust, STP, IT, Global, Market, Peace, Neutral, War.

I. INTRODUCTION

Since 1983, US Department of Defense (DoD) had seen initial wave of globalization and they began emphasizing many defense strategies to protect US interest in the world [1]. To position as world leader in defense technologies, the DoD introduced Multi Level Security (MLS) and it was documented in a series of publications called Rainbow Series. The main book that has been used for reference in computer security area is Trusted Computer System Evaluation Criteria (TCSEC) or called Orange Book [2]. The Orange Book becomes the foundation for Information Technology Security Evaluation Criteria (ITSEC) released in 1990. After that, Common Criteria (CC) standard was introduced based on mutual agreement between World War II countries such as USA, UK, France and Germany. This agreement has been used to standardize the evaluation of security in IT technologies and related products [3].

This paper attempts to discuss some security and trust issues in Common Criteria for the evaluation and certification of IT products and services. It is intended to help manufacturer in choosing the finest authorizing member of CC certification for IT products and services, which would suit varying situational cases such as friendly, neutral and tension situations between members and consumers of CC. Choosing right authorizing CC members can help, among others, reduce cost to trade IT products and related services in global market. Consequently, it will give good impact to countries that do business and market their products if they have wider acceptability of the CC certification. Finally, we illustrate our proposed trust models that adopt game theory in choosing the best CC authorizing member.

II. RELATED WORKS

A. *Trusted Computer System Evaluation Criteria (TCSEC) or Orange Book*

The Orange Book was first developed by United State Government, Department of Defense (DoD) by National Security Agency (NSA). It was the 1985 that had been used to evaluate computer systems and it resources including networking. The purpose of this book is to "*provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies…*"[2]. This book consists of security policy (e.g., mandatory security policy), individual accountability (e.g., identification, authentication and etc.), sufficient assurance (e.g., operation assurance, life-cycle assurance and etc.) and documentation (e.g., trusted facility manual and etc.). To evaluate security criteria, the criterion is classified into 4 classes with priority and classified level.

i. Minimal Protection (Class D), refers to a system that has failed evaluation to meet requirement of upper class (e.g., Class C and above).

ii. Discretionary Protection (Class C) refers to any system that has satisfied Trusted Computing Base (TCB), discretionary security protection (e.g., separation between users and data) and controlled access protection (e.g., audit trials and resource isolation).

iii. Mandatory Protection (Class B) refers to any system that has label security protection (e.g., data sensitivity labels), structured protection (e.g., security policy clearly defined and formally documented) and security domains (e.g., exclude code not satisfies the security policy).

iv. Verified Protection (Class A), for A1) refers to any system that has been verified its design using formal design and verification techniques, to ensure the system can effectively protect classified or sensitive information, which are processed or stored by the system. For beyond A1, system architecture must be formalized and TCB must be verified down to the source code level using formal verification methods. To verify an operating system or a very complex system, validator may use high level language to express system properties with proper consideration of semantics, formal interpretation, mapping and stages of the abstract formal design to formalization of the implementation in low-level specifications.

B. Information Technology Security Evaluation Criteria (ITSEC)

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. Currently, most European countries 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 [3]. Its evaluation focuses on verifying security features identified in Security Target (ST) document. Comparatively, ITSEC evaluation is a little bit different compared to TCSEC because it does not require evaluated target systems to include detailed evaluation in technical design and implementation.

C. Common Criteria (CC)

CC was 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 that signed Common Criteria Mutual Recognition Arrangement (MRA) to recognize CC evaluations for IT security products and services. Malaysia, through CyberSecurity Malaysia was accepted as a consuming participant of Common Criteria Recognition Arrangement (CCRA) on 28th March 2007 [4]. CC was published to unify pre-existing security standard for users, vendors, manufactures (industries) and government in using standard security requirements and evaluations. The purpose of evaluation process is to establish a level of confidence for the security functionality of IT products. The assurance measurement (evaluation criteria) is applied to test against these products and the results may help consumers to conclude whether they meet accepted standard security requirements or fail to meet what they claimed [5], [6]. Figure 1 shows CC evaluation concepts and relationships.

To assess CC assurance levels, various criteria is categorized into 7 classes according to priority and detail evaluation levels [7]:

1. Evaluation Assurance Level 1 (EAL1) – security functionality testing for security functional requirements (SFRs) and it is a basic level of assurance in CC.
2. Evaluation Assurance Level 2 (EAL2) – structural testing for the target system and it requires developer to share their design information and test results for CC evaluations.
3. Evaluation Assurance Level 3 (EAL3) – methodical checking and testing for target system. This evaluation includes environmental control for development of the system.
4. Evaluation Assurance Level 4 (EAL4) – methodical designing, testing and reviewing for target system. Examples of evaluated criteria are security architecture description, automation, and evidence of secure delivery procedures.
5. Evaluation Assurance Level 5 (EAL5) – semi-formal designing and testing for target system. Examples of evaluated criteria are semi-formal design descriptions, a more structured and analyzable architecture and an independent vulnerability analysis demonstrating resistance to penetration attackers with a moderate attack potential.
6. Evaluation Assurance Level 6 (EAL6) – semi-formally verified designing and testing for target system. Examples of evaluated criteria are comprehensive independent vulnerability analysis, improved configuration management and development environment controls.
7. Evaluation Assurance Level 7 (EAL7) – formally verified designing and testing for target system. Examples of evaluated criteria are comprehensive analysis using formal representations (e.g. formal method), formal correspondence, comprehensive testing, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential.

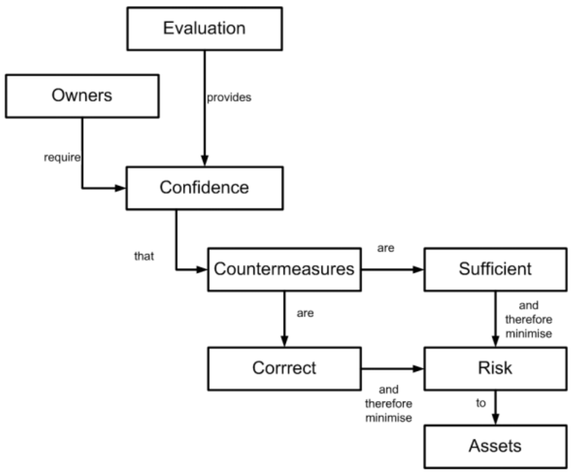

Figure 1: CC evaluation concepts and relationships [6].

D. Related Issues Regarding CC

Many researcher and industry practitioners argued the practicality of CC in a world with rapidly changing situations wherein CC can only exist in its Utopia world [8]. Some of issues are:

i. The lack of interests in buyer and seller because most evaluations and certifications resulting from government regulation or government purchase, and the investment used for CC certifications will substantially increase overall cost and market prices [9], [10].

ii. In theory, mutual recognition amongst nations may save money, resources, and time but the practical effect might fluctuate [8] because of political interest of a nation especially in circumstances of friendly, neutral and war crisis.

iii. Rigid structures and complex process in certifications and evaluations have resulted in tendency to break the practice of CC over time [8], [11].

iv. Trust and policy may change over time, for example, countries may change roles, a new country may joint or leave CC because its national security is at stake and their chain of considerations becomes more selfish and focused on protecting their own interest [8].

v. Software and systems developed by Open Source communities may get left behind and may become obsolete because of lack of funds to support certification process. Consequently, users are forced to use only certified software. This is another form of digital right management (DRM) enforcement.

E. Security, Trust and Privacy (STP)

STP framework can help reduce the many contradictions in these three elements and tighten their relationship using a unified approach to improve security policy and security conduct in protecting user personal and working data [12]. Major concern in STP which involve various stake holders such as systems architect, engineers, designers and developers who are still struggling to create a secure, trustworthy, and privacy preserved environment for us to do business transactions and collaborations. We also noted that currently, STP issues are addressed and alleviated in silos. With forthcoming cloud computing infrastructure being build, we are still facing a big challenge in research work to protect user identity, data and platform wherein all business transaction are being materialized virtually somewhere in the cloud [12].

F. Suggestions for CC Improvements

Kallberg [8] identified trust as an element that is important to ensure that members of CC are able to recognize and consume CC products and services. He argued that "*long-term survival of CC requires abandoning the global approach and instead use established groupings of trust".* His major suggestion was to have customized group of CC based on mutual interest such as defense alliance, economic cooperation agreements, historical events, and political alliances, because it convey transitive trust between its partners. Kallberg viewed from the perspective of relationships and trust boundaries between nations, which he considered as major issues and proposed *group of trust* as a trivial solution for these problems. We agree with Kallberg scheme, however it is not enough to maintain trust relationship between the members because the situation is more complex with three variables of situations: i) friendly (ally), ii) neutral and iii) foe of war (or at war). These circumstances may tear the CC certifications into useless piece of papers after spending a lot of money, time and resources on it.

G. Game Theory

Game Theory is a theoretical framework used for assessment in decision making by individual, group, organization, society and nation. The word *"game"* does not actually refer only to enjoyable games intended for kids or youngsters. The relevance of this theory is that a player (or stake holder) can theoretically gain the best benefit or income through choosing the best action for a specific event or situation [13–15]. Because of its generalized nature, Game theory can be adapted to solve mathematics, economics, political, educations, thinking process and predictions [13], [16]. We believe that the game theory will continue to evolve and help satisfy situational and conditional equilibrium.

Game theory had been studied as early as 1928 by John Von Neumann in "cooperative games" [17]. This publication used Brouwer's fixed-point theorem [18] to evaluate a continuous mappings into compact convex sets as a proof [17]. This proof was used at that time as a standard method in evaluation and decision making in the traditional game theory. Another book in 1948 authored by him and Oskar Morgenstern discussed further cooperative game with many players with *axiomatic theory of expected utility* to treat decision-making under uncertainty. The book *"Theory of Games and Economic Behavior"* [19] helped many mathematical statisticians and economist scholars in decision making using this theory.

By definition, a cooperative game is a game wherein groups of players can enforce contracts or coalitions; therefore the rivalry happens between coalitions of players, rather than between individual players. In some games, it may lead to win-win situation to many players simply because of its probability not being fixed between zero and one (with total product is one). This happens when a game has more than one for the summation of the probability in mixed strategy. However, the term “mixed strategy” can be used only in non-cooperative game because its total product is one (e.g. zero-sum game) as mentioned in John Nash’s theory [20].

Non-cooperative games (1951) was presented by John Nash which discussed the contradiction to Von Neumann’s theory wherein each participant in the game do not perform collaboration, coalition or communication and it assumed that each players acts independently [20]. Major discussion in that paper is the *equilibrium point* or Nash Equilibrium (NE) in a two-person zero-sum game. NE involves two or more players in a game, in which each player is assumed to know the equilibrium strategies or a complete definition how a player will play in that game (pure strategy) [13]. In this game, a player will not benefit by changing only his own strategy individually because the other player will choose the best response by guessing the opponent strategies in the game, due to its pure strategy knowledge for all players in the game.

Zero-sum game can be represented using payoff matrix to assess player’s gains and losses in the game. By definition, *Zero-sum* means, if the total of gains and losses are added up, it will produce a zero value [21]. Players in Zero-sum game try to choose the best strategies to defeat the opponent by minimizing the possible loss for a worst case scenario (minmax strategy). Minmax refers to a part of mixed strategy in zero-sum game used by players in decision making. The mixed strategy means all strategies (pure strategy) in the game had a probability to be chosen by players in the game [20] and that is including zero probability. Players will pick the minmax decision based on *payoff function* which is a mapping of cross product of player’s strategy (gain) with player’s payoff (loses) in the payoff matrix.

We will discuss in more detail regarding the selection for the fines authorizing member of CC certification using game theory in Section V.

III. Research Goal

Our research goal is to propose a new framework for CC evaluations and certifications. Our preceding research works [22], [23] had highlighted some trust problems that are we have identified and we briefly describe them in this paper. Our intention is to have an acceptable and applicable CC in global situations which is dynamically changing in terms of nations’ international relationships, such as friendly, neutral or war. In this research, we begin by identifying suitable case studies that are related to these three situations. This is followed by modeling these situations for better understanding in choosing the finest authorizing CC member for certification process. After that, we try to relate new models with the game theory to further explore the potential applications. Finally, we hope the CC’s certificate can be used globally by many CC consumers wherein it meets the CC’s goal to have a unified certification.

A. Research Objectives

The objective of this research is to help interested stake holders in choosing a finest authorizing member of CC certification for IT products and services using our proposed framework taking into account the dynamically changing international relationship among nations. We suggest to take into account the three states (friendly, neutral or war) as parameters when evaluating CC authorizing member for their IT products and services. These states of trust model can be simulated using finite n zero-sum game.

B. Motivations

The motivation of research is to have stable, consistent and neutral CC authorizing members in evaluation and certification of IT products and related services that may help reduce overall cost of trading IT products and related services in global market. The desirable impact on global business is that businesses and market will become more widely accepted through CC certification.

IV. Proposed New CC Certification Framework

We assumed existing CC members trust the assessments, evaluations (TOE) and certifications wherein each member strictly follows the CC framework. Figure 1 shows the current CC authorizing and consuming members as our main motive. Among the constraints include, for example, not all CC authorizing member has the necessary capability to do TOE for certification up to level 7 or EAL 7. This happens because of difficulty in fulfilling the expertise requirements for high and higher TOE levels. Say, to come out with level 6 or 7, the evaluator and client (manufacturer or vendor) must know a formal representation and evaluation such as formal method in the TOE process.

A. Well-Established Group in the Global

Based on suggestion by Kallberg [8], we identified a few major groups that is well established such as United Nation (UN) [24], European Union (EU) [25], North Atlantic Treaty Organization (NATO) [26], African Union (AU) [27], Organization of Islamic Cooperation (OIC) [28] and Major non-NATO Ally (MNNA) [29]. Each group is founded based on mutual collaboration and interest in certain areas such as economy, human welfare, military, education, geographical location, historical events, financial and joint venture to fight against terrorism. Figure 2 shows major groups and some of their respective members. These groups may take advantage of their good relationship amongst themselves to become the finest authorizing member of CC certification based on their mutual interest.

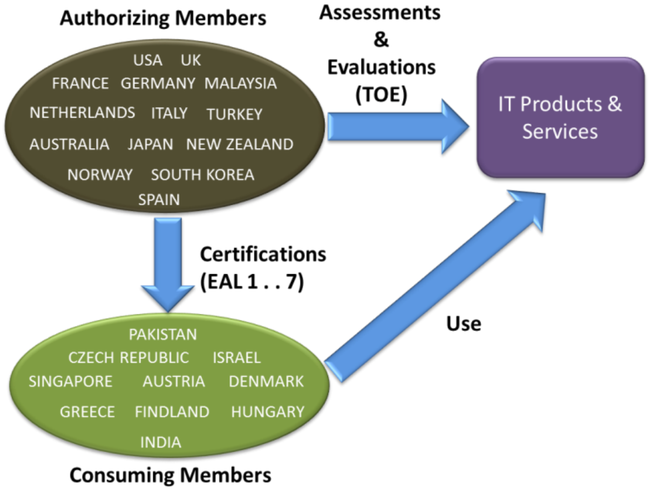

Figure 1: Current CC's Authorizing and Consuming Members [5].

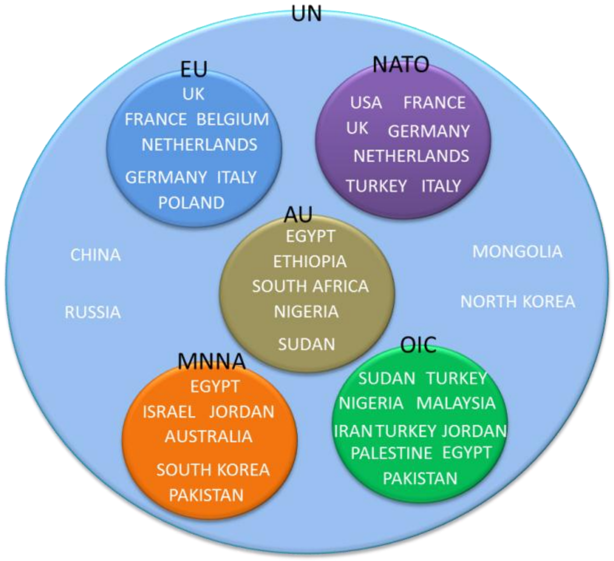

Figure 2: Examples of well-established groups and it members.

B. *An Overlapped Memberships in the Group*

To enhance Kallberg [8] proposal, we may use interception memberships between group as bridge to connect and expand the CC framework to cover broader scope as shown in figure 3. A nation with multiple memberships can be a better option to choose as CC authoring member, for example, because of the nation's wider coverage to offer CC certification and has better transitive trust between its partners in the group. For instance, NATO and EU groups can employ UK or FRANCE as their CC authoring member within these two groups. However, there is no guarantee that these overlapping membership nations will maintain their original state forever. Such situation may exist when the nation changes its state. This also means that the idea of grouping and overlapping the grouping is not good enough to make CC framework work in reality.

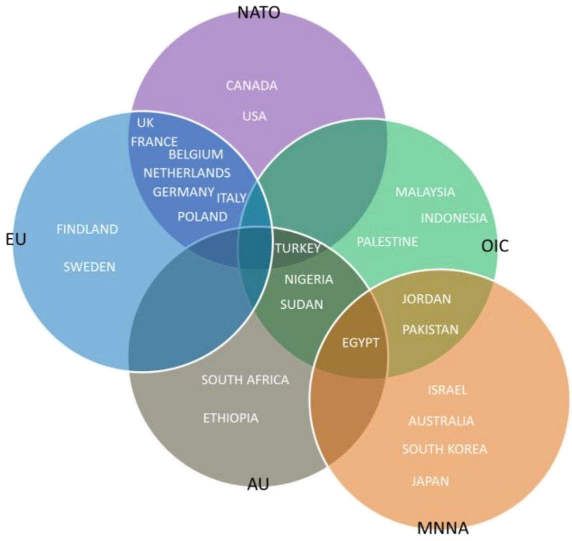

Figure 3: An overlapped memberships in different groups.

C. *Trusted Framework for CC*

We may now have the impression that CC framework as described above is impracticable. However, we view that the framework can be further enhanced by adding *trust* mechanism into the framework. However, trust is not a constant, rather a variable that change over time because of other factors. This is where Trusted Computing (TC) can help resolve trust issues. The basic idea behind TC is to have Trusted Platform Modules (TPM) which is a chip, that acts as the basis of trust, called *root of trust* for all processes, transactions or communication [30–34]. Currently, the TC specifications have not even achieved up to EAL level 5. Regarding Kallberg [8] comment that ultimately CC framework can be only exist in Utopia, we would like to give our alternative view to solve it.

We propose that the framework solve trust problem by optimizing the process of choosing CC authoring member to do TOE in our IT products and services. We divide member nations into 6 categories to be used for the optimized choosing algorithm for an ideal CC authoring member for TOE process, described as follows:

i. *Perfect* condition wherein each entity is in friendly or ally relationship as shown in figure 4.

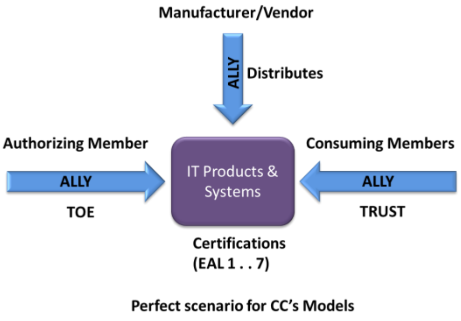

Figure 4: Perfect relationship.

ii. *Distorted* condition wherein, while authorizing member and manufacturer entities are both in friendly or ally relationship, on the other hand, the consumer is in neutral relationship with both entities as shown in figure 5. This situation also applies to the condition where authorizing and manufacturer entities are in bad relationship.

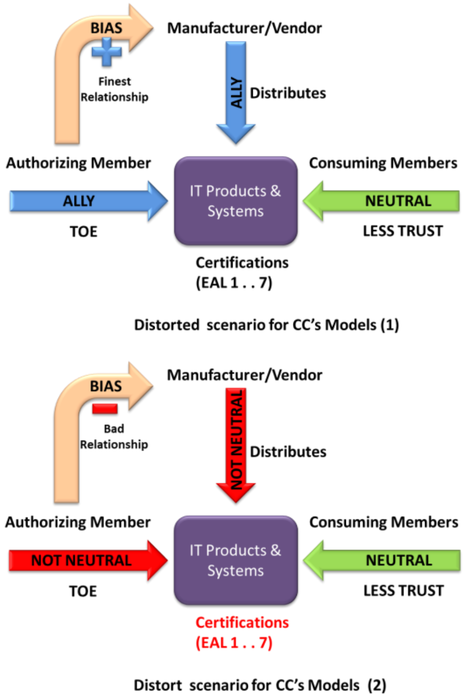

Figure 5: *Distorted* relationship.

iii. *Impossible* condition wherein each entity is in bad relationship with another entity as shown in figure 6.

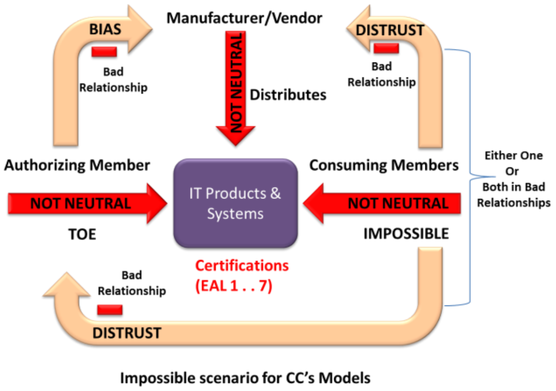

Figure 6: *Impossible* relationship.

iv. *Almost Impossible* condition wherein consumer entity is in bad relationship with authorizing or manufacturer entities or may be both as shown in figure 7.

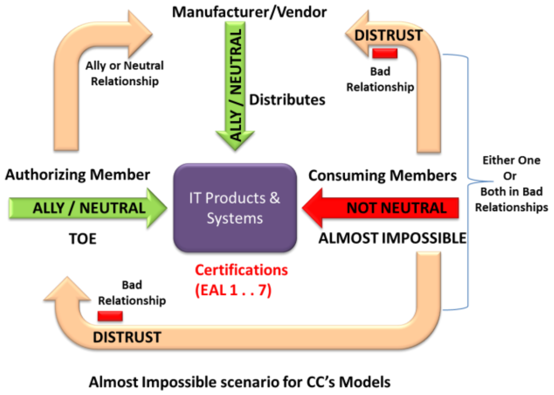

Figure 7: *Almost Impossible* relationship.

v. *Neutral* condition wherein each entity is in *Neutral* relationship with another entity as shown in figure 8.

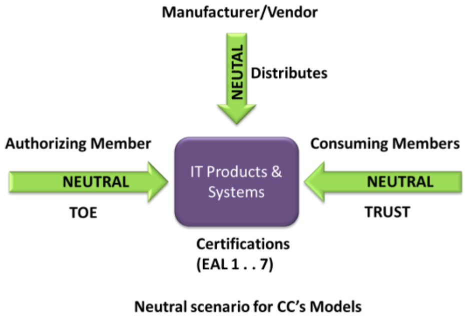

Figure 8: *Neutral* relationship.

vi. *Positive* condition wherein consumer entity is in ally relationship with authorizing or manufacturer entities as shown in figure 9.

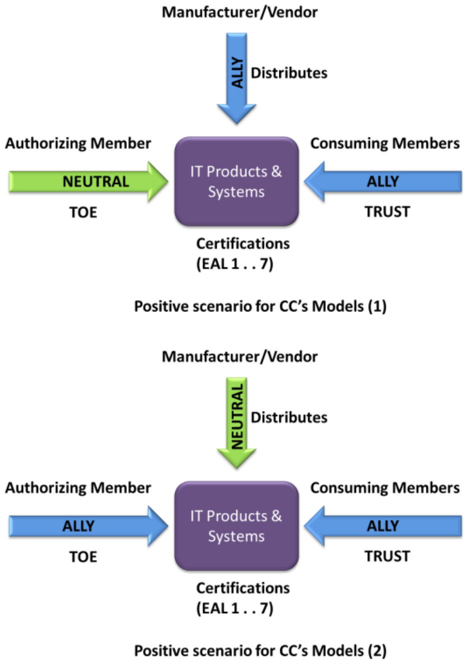

Figure 9: Positive relationship.

V. DISCUSSIONS

We propose to use overlapping memberships between groups as the bridge to connect and expand CC framework and also to identify the optimized CC authorizing member to do TOE in our IT products and services. However, it is very difficult to evaluate or to measure *trust* and then to maintain it from changing over a period of time. *Trust* can be built and or broken because of changing circumstances. We have presented some possible relationships that may affect the CC certification. Choosing proper entities in the evaluation process such as neutral, positive, perfect relationships can potentially help to reduce *trust* problem. We intend to study more on this area of research.

A. Trust Model

At the moment, we have done performance measurement of overlapping memberships of CC which is counted based on number of countries that are in the group and the overlapped group. For example, Egypt has higher potential to be finest CC authorizing member because this country is a member of a few groups i.e. AU, MNNA and OIC. All members of these three groups can utilize Egypt's TOE as trusted third party for CC certification. For another example, based on figure 3, Indonesia (OIC member) can market their product in Japan (MNNA member) because of both countries have good relationship with Egypt (with memberships in AU, MNNA and OIC). With reference to Kallberg who argued *"The utility with using groups with established trust structures are the obvious - the trust is in place"* [8]. We believe that each member of the group had some kind of mutual understanding and trust agreement that makes it best for them to be in the group. Therefore, choosing a country with many memberships as CC authorizing member can help manufacturer or vendor to attain wider market for them to export IT products and services. It can also help in avoiding impractical situations such as those cases of Distorted (Figure 5), Impossible (Figure 6) and Almost Impossible (Figure 7) situations in CC models. We summarize our trust models as shown in Table I.

TABLE I. PROPOSED TRUST MODELS FOR INTERNATIONAL RELATIONSHIP IN COMMON CRITERIA EVALUATION & CERTIFICATION.

State	*Relation*	*Rational Decision*
S1	NEUTRAL ^ NEUTRAL	TRUST
S2	ALLY ^ NEUTRAL	TRUST
S3	ALLY ^ ALLY	TRUST
S3	WAR ^ NEUTRAL	NOT TRUST
S4	WAR ^ ALLY	NOT TRUST
S5	WAR ^ WAR	NOT TRUST
S6	NEUTRAL v NEUTRAL	TRUST if either S1,S2 or S3
S7	ALLY v ALLY	TRUST if either S1,S2 or S3
S8	WAR v WAR	NOT TRUST
S9	∴ If WAR in any relation	NOT TRUST
^ relationship between manufacturer and CC authorizing member with consumer v relationship between manufacturer and CC authorizing member		

B. Game Theory

Before adopting the game theory for choosing the best CC authorizing member, we must first identify the type of games, actors (players), strategies (pure strategy and mixed strategy) and payoff function for all n-games. Considerations include constructing an initial design, studying its main principles; then, we need to find dominance strategy for all players in the n-games. The dominance strategy refers to a common rational decision made by rational people in choosing the best action for certain event or situation. In essence, many simple games can be solved using dominance strategy. Its main objective is to lead the player to be the winner, no matter how the opponents may play in the game. For our research study, we can choose from several options; cooperative, non-cooperative, zero-sum or non-zero-sum game.

In this paper we present a simple example to illustrate the game theory. We choose to have simple game with the least complexity, i.e. a two-player zero-sum game with matrix 2x2 as shown in Table II. This game represents a competition between two countries (for example, Italy and Turkey) that are CC authorizing members. Assuming both countries want to attract a vendor to certify their IT product for CC certification. In this example, a vendor may have different market target for they product, say western region or eastern region. Initially in this game, we excluded the trust model relationship and we consider only group membership and interception memberships between groups.

TABLE II. TWO-PLAYER ZERO-SUM GAME IN CHOOSING THE BEST COMMON CRITERIA EVALUATION & CERTIFICATION.

Option	*A (Western Region)*	*B (East Region)*
1 (Western Region)	**0 , 0**	**-3 , +3**
2 (East Region)	**+9 , -9**	**-4 , +4**
RED (A & B) Turkey's Strategies **BLUE (1 & 2) Italy's Strategies**		

The game proceeds as follows: The first player (Italy), do not know Turkey's selection. Italy chooses in private either one of the two actions 1 or 2. The second player (Turkey), unaware of the Italy's choice, chooses in private either one of the two actions A or B. Consequently, the choices of both countries are revealed and each country's total point is calculated using a payoff matric based on these choices. The value in the payoff matric is essentially the number of member countries that are in a group and interceptions between members in the group.

In this game both players know the payoff matrix (as in Table II) based on pure strategy and attempt to maximize the number of their gains based on minmax theorem. In this example, Turkey could follow the following reasoning: "With option 1, Turkey could lose up to 9 points and can win only 0; while with action 2, Turkey lose nothing but can win up to 4, so option 2 looks a lot better." Using similar rational, if Italy choose action 1 and Turkey choose option A, Italy will win 9 points. In this illustration, the dominance strategy in this game is to choose options 2 and Turkey will be the dominant player if the similar game is played again. We will do a further study on the game theory, and we will propose an enhance model to finally use game theory for the finest CC Authorizing member selection.

VI. CONCLUSION

In this paper, we have discussed issues related to Common Criteria in evaluation and certification of IT products and services. We intention is to assist manufacturer in choosing the best authorizing member for CC certification for IT products and services in politically dynamic situations amongst countries participating in the CC certification. We have considered three states namely, friendly (ally), neutral and tension (war) situations between members and consumers of CC as parameters in evaluation process for choosing the best authorizing member to evaluate IT products and services. In this preliminary study, we have identified a few trust models that can be used for trust assessment of CC memberships which is counted based on number of countries that are in the group and the interceptions within the group. Finally, we enhanced the trust models further by introducing game theory to identify the best CC authorizing member which principally uses the dominance strategy.

VII. ACKNOWLEDGEMENT

The authors would like to thank to Ministry of Higher Education (MOHE) and Universiti Putra Malaysia (UPM) for providing the research grant (LRGS) for this research work.

REFERENCES

[1] U. S. Military, D. Mackenzie, and G. Pottinger, “Mathematics , Technology , and Trust : Formal Verification , Computer Security ,” vol. 19, no. 3, 1997.

[2] US Department Of Defense (DoD), “Trusted Computer System Evaluation Criteria,” in *Rainbow Books*, 1985, pp. 1–116.

[3] ITSEC Members, *Information Technology Security Evaluation Criteria (ITSEC)*, no. June. 1991, pp. 1 – 171.

[4] Malaysia Government, “Malaysian Common Criteria Evaluation and Certification,” 2011. [Online]. Available: http://www.cybersecurity.my/mycc/about.html.

[5] Common Criteria Members, “Common Criteria for Information Technology Security Evaluation,” 2011. [Online]. Available: http://www.commoncriteriaportal.org/.

[6] Common Criteria Members, “Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model July 2009 Revision 3 Final,” no. July, 2009.

[7] Common Criteria Members, “Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components July 2009 Revision 3 Final,” no. July, 2009.

[8] J. Kallberg, “Common Criteria meets Realpolitik - Trust, Alliances, and Potential Betrayal,” in *IEEE computer Society Digital Library, IEEE Computer Society,*, .

[9] J. Hearn, “Does the common criteria paradigm have a future?,” in *Security &amp; Privacy, IEEE*, 2004.

[10] K. Beatty, “Research paper : Common Criteria Mutual Recognition,” in *Science Applications International Corporation, Common Criteria Testing Laboratory,*, 2007, pp. 1–9.

[11] M. Razzazi et al., “Common Criteria Security Evaluation: A Time and Cost Effective Approach,” in *2006 2nd International Conference on Information & Communication Technologies*, vol. 2, Ieee, 2006, pp. 3287–3292.

[12] Jamalul-Lail Ab Manan , Mohd Faizal Mubarak, Mohd Anuar Mat Isa , Zubair Ahmad Khattak, “Security , Trust and Privacy – A New Direction for Pervasive Computing,” *Information Security*, pp. 56–60, 2011.

[13] M. D. Mccubbins, M. Turner, and N. Weller, “The Mythology of Game Theory,” in *Social Computing, Behavioral - Cultural Modeling and Prediction: Lecture Notes in Computer Science Volume 7227, SPRINGER*, 2012, no. 1, pp. 1–8.

[14] D. Bauso and J. Timmer, “Robust dynamic cooperative games,” *International Journal of Game Theory*, vol. 38, no. 1, pp. 23–36, Aug. 2009.

[15] S. Alpern and S. Gal, “Analysis and design of selection committees: a game theoretic secretary problem,” *International Journal of Game Theory*, vol. 38, no. 3, pp. 377–394, Apr. 2009.

[16] R. B. Myerson, “Game Theory: Analysis of Conflict,” 1991.

[17] J. V. Neumann, “Zur Theorie der Gesellschaftsspiele (On the Theory of Games of Strategy),” *Mathematische Annalen*, pp. 295–320, 1928.

[18] L. E. J. Brouwer, “Brouwer fixed-point theorem,” *WikiPedia*, 2012. [Online]. Available: http://en.wikipedia.org/wiki/Brouwer’s_fixed-point_theorem.

[19] Von Neumann and O. Morgenstern, “Theory of Games and Economic Behavior,” 1944.

[20] J. F. Nash, “Non-Cooperative Games,” in *The Annals of Mathematics*, 1951, pp. 286–295.

[21] J. W. Mamer and K. E. Schilling, “A Zero-Sum Game With Incomplete Information And Compact Action Spaces,” *Mathematics of Operations Research*, vol. 11, no. 4, pp. 627–631, 2012.

[22] Mohd Anuar Mat Isa Anuar, Habibah Hashim, Jamalul-lail Ab Manan, Ramlan Mahmod, Hanunah Othman, “Finest Authorizing Member of Common Criteria Certification,” in *The International Conference on Cyber Security, CyberWarfare and Digital Forensic 2012 (CyberSec12)*, 2012, pp. 166–171.

[23] Mohd Anuar Mat Isa, Habibah Hashim, Jamalul-lail Ab Manan, Ramlan Mahmod, Mohd Saufy Rohmad, Abdul Hafiz Hamzah, Meor Mohd Azreen Meor Hamzah, Lucyantie Mazalan, Hanunah Othman, "Secure System Architecture for Wide Area Surveillance Using Security , Trust and Privacy (STP) Framework," *International Journal of Procedia Engineering*, no. International Symposium on Robotics and Intelligent Sensors 2012 (IRIS 2012), 2012.

[24] UN, "United Nation," 2012. [Online]. Available: http://www.un.org/en/members/index.shtml.

[25] EU, "European Union," 2012. [Online]. Available: http://europa.eu/about-eu/countries/index_en.htm.

[26] NATO, "North Atlantic Treaty," 2012. [Online]. Available: http://www.nato.int/cps/en/SID-9E18D6D4-4BA68B89/natolive/nato_countries.htm.

[27] AU, "African Union," 2012. [Online]. Available: http://www.au.int/en/member_states/countryprofiles.

[28] OIC, "Organization of Islamic Cooperation," 2012. [Online]. Available: http://www.oic-oci.org/member_states.asp.

[29] MNNA, "Major non-NATO Ally," 2012. [Online]. Available: http://en.wikipedia.org/wiki/Major_non-NATO_ally.

[30] Mohd Anuar Mat Isa, Jamalul-lail Ab Manan, and Raja Mariam Ruzila Raja Ahmad Sufian, Azhar Abu Talib, "An Approach to Establish Trusted Application," in *2010 Second International Conference on Network Applications, Protocols and Services*, 2010, pp. 159–164.

[31] Mohd Anuar Isa Mat, Azhar Abu Talib, Jamalul-lail Ab Manan, and Siti Hamimah Rasidi, "Establishing Trusted Process In Trusted Computing Platform," in *Conference on Engineering and Technology Education, World Engineering Congress 2010*, 2010, no. August.

[32] TCG Group, "TCG specification architecture overview," in *TCG Specification Revision 1.4*, no. August, 2007, pp. 1–24.

[33] Sharifah Setapa, Mohd Anuar Mat Isa, Nazri Abdullah, and Jamalul-lail Ab Manan, "Trusted computing based microkernel," in *Computer Applications and Industrial Electronics (ICCAIE 2010)*, 2010, no. Iccaie, pp. 309–312.

[34] L. H. Adnan, H. Hashim, Y. M. Yussoff, and M. U. Kamaluddin, "Root of Trust for Trusted Node Based-on ARM11 Platform," 2011, no. October, pp. 812–815.