Abstract— Globalization had changed the world landscape into borderless world without limits to sea, land and air space. The development of IT products and services need evaluation and certification. This paper discusses some security and trust issues in Common Criteria in evaluation and certification of IT products and services. Our intention is to help manufacturer in choosing a finest authorizing member of CC certification for IT products and services in varying situations amongst countries participating in the CC certification, be it friendly, neutral or war. The consequence is to help reduce cost to trade these IT products and related services in global market. The ultimate impact is to enable us do more business and market our products in other countries if we have wider acceptability of the CC certification.

Keywords – Common Criteria, CC, TCSEC, ITSEC, Security, Evaluation, Assessment, Trust, Privacy, Verify, STP, IT, Global.

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 became 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.

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), discretion 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.

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].
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.

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

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].

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 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.

III. RESEARCH GOAL

Our research goal is to propose a new framework for CC evaluations and certifications. 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. 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.

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) [13], European Union (EU) [14], North Atlantic Treaty Organization (NATO) [15], African Union (AU) [16], Organization of Islamic Cooperation (OIC) [17] and Major Non-NATO Ally (MNNA) [18]. 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.

![Diagram](image1.png)

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

**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.

![Diagram](image2.png)

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

![Diagram](image3.png)

**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 [19–23]. 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:

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

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

Figure 6: Impossible relationship.

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

Figure 7: Almost Impossible relationship.

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

Figure 8: Neutral relationship.

v. **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.

At this stage, 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 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.

VI. CONCLUSION

This paper discussed issues in Common Criteria in evaluation and certification of IT products and services. We would like to help manufacturer in choosing a finest authorizing member of CC certification for IT products and services in varying situations amongst countries participating in the CC certification, be it friendly, neutral or war. 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 finest authorizing member to evaluate IT products and services. We intend to study this area of research using modeling and formal verification methods.

VII. ACKNOWLEDGEMENT

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

REFERENCES