Selected Papers in Security Studies: Volume 9

Common Criteria Meets Realpolitik
Trust, Alliances, and Potential Betrayal

Technical Report UTDCS-13-12
The University of Texas at Dallas
Department of Computer Science
August 2012

Jan Kallberg

Selected Papers in Security Studies: Volume 9

Common Criteria Meets Realpolitik

Trust, Alliances, and Potential Betrayal

Jan Kallberg
CySREC, Erik Jonsson School of Engineering and Computer Science
The University of Texas at Dallas
Richardson, TX 75083-0688
jkallberg@utdallas.edu

This is the ninth in a series of reports we are writing on Security Studies and the application of information technology for providing security and combating terrorism. We will include papers on both cyber security and national security. The purpose of these series of reports is to guide us in the technologies we are developing for both cyber security and national security. The technologies include systems for assured information sharing and assured cloud computing and tools for secure social network analysis and data mining for security applications such as malware detection. Our research to develop these technologies is supported by the Air Force Office of Scientific Research.

DISCLAIMER: The Views and Conclusions contained in this report are those of the author and do not reflect the policies and procedures of the University of Texas at Dallas, the United States Government or the Air Force Office of Scientific Research.

Abstract— Common Criteria for Information Technology Security Evaluation has the ambition to be a global standard for IT-security certification. The issued certifications are mutually recognized between the signatories of the Common Criteria Recognition Arrangement. The key element in any form of mutual relationships is trust. A question raised in this paper is how far trust can be maintained in Common Criteria when additional signatories enter with conflicting geopolitical interests to earlier signatories. Other issues raised are control over production, the lack of permanent organization in the Common Criteria, which leads to concerns of being able to oversee the actual compliance. As Common Criteria is formulated today it is unlikely that it would survive over time. The reasons why it might fail are the rigid framework, rapid technical development makes a security target a moving target leading to instability and uncertainty, and the increased militarization in cyberspace moving from information assurance to information operations.

Keywords - common criteria; trust; nation state; coalition; NATO; information security; conflict; war; CCRA

I. INTRODUCTION

Common Criteria for Information Technology Security Evaluation (CC) has a long history starting in the 1980s as the United States Department of Defense's Trusted Computer System Evaluation Criteria [1] that merged with the European Information Technology Security Evaluation Criteria (ITSEC) [2][3] in the late 1990s to reach its final form as CC [4]. The idea is that once an IT-security product is certified as secure to use, the certification is mutually recognized within a group of signatories of the Common Criteria. The users drive the process by defining functional and assurance requirements, the vendors meet these requirements and the certification laboratories can then validate the implementation and certify the products so the users can be assured. The CC standard has been accepted as an international standard ISO/IEC 15408. There are two types of signatories: authorizing and consuming members of CC. The authorizing members can issue and accept issued CC certifications; meanwhile, the consuming members can only accept CC certifications but not issue.

The functional requirements and the processes that are defined as being necessary to protect the system or hardware form the Protection Profiles (PP)[5]. These requirements and processes are gathered by CC user groups, in several cases agencies associated with the national military establishments, and depending on the function these protection profiles can be over ten years old. The fact that the functional requirements are generated by a federal and military community also presents a challenge for civilian use and the perception of functionality could be different between these user groups. The PP are broken down to Security Targets (ST) that specify the security properties and can be relevant to several PP and are not specific for one profile.

In the certification process a level of evaluation is established by rating of the Target of Evaluation (TOE), which can be a product or system, and is provided by an Evaluation Assurance Level (EAL) ranking from 1 – 7 where 7 is the highest level. The EAL is an indication of how rigorous the verification process has been and not a measurement of actual security that the TOE provides [6]. At the lowest EAL levels, the evaluation is an ocular review of the design and documentation.

An immediate concern is how up-to-date the less central parts of the CC certification process are. The PP for Automatic Teller Machines (ATM) is from 1999 and for postage meters 2001. The PP for voting machines is dating back to 2006. These machines might not matter to the institutional users that form authors of the PP repository, but for the general population it is favorable to at least have secure ATMs and voting machines.

The definition of PP and the actual authorship of the CC requirements and documentation are done by government-related groups and agencies with marginal input from the industry. The lack of input from industry and commercial interests undermines the adaptive approach needed to maintain CC's relevance over time and also explain the limited interest from the industry [7]. Industry with their own research departments are in many cases the first to see flaws in their own and competitors' products.

II. Mutual Recognition and Trust

Trust is pivotal for the success of CC, especially with the ambition to be a world standard where countries mutually recognize security certifications issued in foreign countries. The methodology is outlined in Common Methodology for Information Technology Security Evaluation (CEM). Together with CC comes an agreement of mutual recognition: Common Criteria Recognition Arrangement (CCRA) which ensures that specific technical requirements are met according to the CC and is an agreement between the entering state and the states that are already members of CC. In an ideal world, the need for internal certification and control in countries that buy IT-security equipment would be removed as they now can trust the authorizing countries' laboratory that the goods are safe from a security standpoint. The vendor A1 can certify the equipment in country A, and sell the equipment to buyer B1 in the country B, because the countries A and B trust each other and the process works in reverse order when B2 certifies a product in B to sell to A2 and so on. A and B mutually recognize the certification made in country A or B. This solves other issues as A1 does not have to show the source code for B to certify thereby avoiding any leakage, national security concerns, and export compliance. This has a long-term importance if there are tensions or distrust between A and B later. Mutual recognition saves money, resources, and time in theory but the practical outcome might differ.

It is important to see CC as a product in itself added to the basic equipment and treat it accordingly. If CC works, it should enhance security and increase assurance that the equipment that is procured is safe and ready to use. The membership circle of CC is limited and could be seen as NATO and friends. The countries that have signed on the CC are either NATO countries, aligned with NATO or the U.S. The only outlier is Malaysia as an authorizing country. Consuming countries are different as they do not authorize but accept certified products and as only buyers and users, the trust issues are less significant. Consuming and accepting a certificate requires trust, but the level of trust that is needed to originate certificates is far higher. A consuming country can have buying preferences; meanwhile, an authorizing country is accepted by all.

In a world that is ever changing, rigid frameworks tend to break over time. CC has benefits but the institutional design raises several questions over its long-term impact, survivability, and abilities. Trust can change over time even in the most rigorously designed institutions of international or regional cooperation and roles assigned can be mis-managed. International institutions' rules and bylaws, even if they are voluntarily and loosely bound together, are complex and face their largest challenge in changes of the initial conditions over time.

Once an international institution is formed, it is often less adaptive to an ever ongoing evolution in the outer environment. It is nothing unique for Common Criteria; it has plagued interstate cooperation for centuries. As time goes by, actors change roles and new actors enter; a trust is won and lost. First, one of the core motivations for CC is easiness and removing regulatory hurdles and redundancies. Ideally, CC saves money for the parties that trust each other and can maintain the trust. Each state does not have to certify every single IT-security tool and hardware that enters the market. The number of states that are potential signatories of CC make it an opportunity to save money, time to market, and standardize IT-security by removing redundancy in assurance.

In areas of mutual political understanding such as European Union, it makes sense. If there are no geopolitical tensions, violent cleavages, and a significant degree of political coercion, CC is useful coordinate IT-security certifications. If there was no coordination between the EU 27 member states, a vendor should be forced to certify equipment in each country and best practices would be lost in a regulatory fog of war. Once a product is certified, it receives a license that will be mutually recognized in other countries in the CCRA framework, without which, the manufacturer has to supply source code and other technical information to each of these countries for certification purposes.

In the light of political realism, we have to face the alternative force. Authorities, agencies, and the defense establishment are organizations that need to justify their existence and claim territory whenever a new field opens up in their arch of influence. For a manufacturer of IT-security hardware, it can turn into a nightmare because Internet security affects many regulatory realms. Problems well-stirred can be seen from the fields of consumer protection, financial regulators, law enforcement, defense, emergency management, and all the way to trade commissions. Some issues are real; others are pure bureaucratic maximization. If not coordinated, it represents a regulatory tsunami. The final entropy is if these agencies are setting their own standards and technical specifications. The theoretical regulatory nightmare is a strong case for the implementation of CC. The first consideration must naturally be if it improves security.

III. IDEALISM VERSUS REALPOLITIK

A quote from Kenneth N. Waltz [8] comes to mind: *"A lot of people don't like realists. Realists face the world as it is. Most people want the world to be nicer and for people to be better."* CC is a voluntarily association and it is up to each state to apply to be a member and sign the agreement that details the requirements, obligations and mutual recognition. CC is a detailed and technical framework where details have been studied and weighted. Politics operate differently.

Security in a political context is a notion – a feeling. Politics decide national security agendas. The question is what happens when the states' national security interests are at stake and their chain of considerations becomes more selfish and focused on protecting their own interest. The militarization and presence of covert cyberwar give a deviating CC actor a *carte blanche* to manipulate and create opportunities to exploit. Mutual recognition with countries that are not closest allies makes many policymakers uncomfortable. The slightest distrust catalyzes second thoughts and questioning. A reflection regarding CC is if the concept is stuck in the euphoric days after the collapse of the Soviet Union and sprung out of the decade of decreasing conflicts and increasing cooperation between nation states that followed the end of the Cold War. Today the trajectory has slowly and incrementally been reversed with increasing conflicts and less cooperation.

When cyberspace becomes a part of the military realm and integrated in national defense strategies, one of the words that comes to mind is control. It is central for any defense strategy to achieve and maintain control of the operation area and if cyberspace becomes a part of the battlefield, then cyberspace is no different than territorial waters and sovereign air space. The control needs to be extended not only to the battlefield, but also to the resources and abilities at hand to fight the battle. Mutual recognition is limiting control and instead giving away control. The militarization of cyberspace raises the threshold for trust [9] [10] and an increasing complexity in infrastructure and equipment defuse a sense of control and undermine trust. It is also questionable if CC will be able to adapt to the radical shift in cyber warfare from solely defending infrastructure through information assurance to an environment that is pursuing aggressive information operations. *Cyberwar as the new warfighting domain would increase the interest of national control – instead of usher in an era of mutual trust based on laboratory reports from a foreign country.*

These two drivers, the militarization and increasing complexity, are working against a wider implementation of CC. Internet infrastructure is an important asset in the conflict between powers. Realpolitik is pragmatic. There is more life in CC than just sudden death at the moment of distrust. National security can live with limited distrust if there are other means of trust, if there is a history of trusted cooperation, and there is a political deterrence through other engagements for defection of any counterpart. The solution is hidden in how CC is organized and structured. Today all countries are in one global pool and CC is targeting global signatories. I argue that the long-term survival of CC requires abandoning the global approach and instead use established groupings of trust.

IV. FUNDAMENTAL CONCERNS

Mutual recognized certifications should survive political and geopolitical sentiments. If not the trust is no longer there and nations could start to disregard the certification by covertly recertifying or refusing to buy equipment that raises concerns even if mutually recognized, and the CC certificates carry no value. If conflict increases and tension rises between nations, a mutual recognition that goes across geopolitical boundaries and conflict lines will not survive. Let us raise some other concerns a policymaker can put forward.

The CC is designed on the assumption that certification laboratories are completely independent and that no authority can exercise undue influence [11]. Several of these laboratories are small businesses. If CC expands to numerous countries, and especially the Third World, these independent laboratories will be of even smaller scale as the market is less developed. Several of these countries are not democracies which can lead to a vocal government interest in the outcome of the certification.

In a utopian world where everyone shares the same goal, belongs to the identical geopolitical cluster, and kindness is the prevailing political outlook, independence might be true for all. Without dwelling on the fact that this planet tends to operate differently, distrust can be injected and undue influence executed. Those conditions are limitations on how far CC can grow. A vendor can choose any certification laboratory of their choice to facilitate the certification. Undue influence can occur when the state where the production is situated pressures the vendor to seek certification at specific laboratories. These laboratories could be in the realm of influence of the specific state where the equipment is manufactured. An additional concern is who has the final control over the production and can influence the manufacturing. An example would be a router that is designed in the U.S., marketed and a product of a U.S. corporation, but the router is made in a factory in China. The subcontractors to the product can be spread over five – ten countries all over the Asian continent. The buyer can be a third country and the product could never enter the

territory of the certificate issuing state. In an example with a European manufacturer, the sourcing becomes even more global as it is likely to involved procurement from Europe, North America, and Far East. The control of the production is beyond of the scope of CC but still crucial to maintain trust.

National security has to be seen with the eyes of a layman because policymakers are not technical formalists but instead non-technical generalists. If the product is certified by a U.S. vendor using a U.S. laboratory and then manufactured in China and shipped directly from China to a third country, why should the policymaker in the third country believe that the U.S. certification is still valid? The reverse example does not work because China is not a member of CC. The example shows the issue and does not single out China *per se*.

Who can guarantee a product that they do not control the production of – especially when parts of it are made in countries with semi-authoritarian regimes or a history of corruption? Another aspect is software updates and soft controls which have a direct impact on the hardware after it enters service post-certification. If non-digitally signed updates are allowed, malicious updates or covert software can nullify the security certification. Mutual recognition is surrendering control to those you trust. The rationale for this surrender must be a proof that the certification process is properly handled.

We cannot ignore politics, even if technicians tend to only see to the technical aspect, because mutual recognition is a highly political agreement between states, especially when cyberspace is militarized and an increasing national interest comes into play. The political aspect can be downplayed, but it is a permanent fixture in any CC and CCRA consideration, especially between countries that do not subscribe to the same geopolitical community of interest and alliance.

The absence of a permanently staffed CC/CCRA organization which is able to conduct validating inquiries on their own initiative and expense on a frequent basis is a weakness in the CC concept. Security is mainly perception. As Internet and the Internet infrastructure become a part of the military and political realm, a centrally staffed organization becomes an understandable counterpart and political interface. This would also increase the accountability for the framework and especially for those who have entered the CCRA agreement. Politicians and national security executives prefer an international organization with a permanent structure and staff. This is the way they are used to conducting business – and that is one reason why Internet Corporation for Assigned Names and Numbers (ICANN) gets leverage. They are staffed and have an international office. It is an interface that the politicians and government executives expect – to some it sounds spurious but it carries the same underlying rationale as wearing a suit at an interview. Those we meet at the interview expect it and we play along to increase our opportunity. Additionally, a more institutionalized CC with budget and management would also be open to the opportunity to fund certification of Open Source software that has no vendor behind it. Otherwise, Open Source would be not accessible for users that are required to only use certified software.

The world has different groups that share interest and outlook on world events, often unified in a custom union, defense alliance, or economic cooperation agreement, just to name a few – European Union (EU), North Atlantic Treaty Organization (NATO), African Union (AU), and Union of South American Nations (UNASUR). The utility with using groups with established trust structures are the obvious – the trust is in place. There are mechanisms to enter, there are funded oversight institutions within these institutions, and there are mechanisms to remove a member or block access to part of the cooperation.

The important difference is not only the long-lasting cooperation between these groups but also the political deterrence of any defection of the actual standard. An alternative is that the countries themselves start to grade the mutual recognition according to trust. One example is the Communications-Electronics Security Group (CESG)[12] of the UK government, which clearly states "CESG also recognises Common Criteria Certificates up to EAL4 issued by Australia, New Zealand, Canada and USA. In addition, certificates up to EAL7 issued by European partners are accepted in the UK." Trust is binary, either you have it or you do not, and it is a sign of weakness that trust has to be graded.

The League of Arab States (Arab League) has 22 member states which are predominantly Sunni and have fostered a relationship with each other for decades. They share religion, history, ethnicity to a degree, language, and have built trusted relationships with each other through the years. The Arab League has mechanisms to address lack of cooperation, disapproving from other members, and distrust between members. Could the Arab League form their own subgroup of CC "Arab Common Criteria" with their own Arab CC, Arab CEM and Arab CCRA? Yes, because once there is a circle of trust, CC could be successful. It does not mean that the member states of the Arab League trust each other blindly, but enough to conform to Arab CCRA between each other. In reality, the CC in its different regional flavors will match the geopolitical patterns of the world and nations can either join, leave, or get removed from the regional CC. These subgroups of CC could be overlapping or standards could be adopted by others as they please.

V. CONCLUSION

We have also to recognize the limitations for CC. The main purpose for CC is "to eliminate the burden of duplicating evaluations of IT products and protection profiles". Therefore, the security outlook has to be aligned with political alliances because they carry inherent trust. Only by accepting the trusted relationships that already exist can CC thrive. The national interest prevails over the international interest if there is a conflict between these interests. Why should any nation trust an IT-security certification from a potential adversary? It is a relevant question. And if we do not allow potential adversaries into the CC, then CC

will never grow further. As cyber warfare goes from information assurance to information operations where the arsenal is covert digital operations initiated by highly funded state actors, it is unlikely that CC as a global certification platform will reach critical mass. The trust will not be there. CC will survive as a certification for NATO and allies – and even then it incrementally can be irrelevant, obsolete and diminish over time.

[1] Powanda, E.J., Genovese, J.W.; "Configuring a trusted system using the TNI," Aerospace Computer Security Applications Conference, 1988., Fourth , vol., no., pp.256-261, 12-16 Dec 1988.

[2] Wood, J., "European harmonised IT security evaluation criteria," Application of Standards for Open Systems,1990., Proceedings of the 6th International Conference on the , vol., no., pp.138-143, 2-4 Oct 1990.

[3] Jahl, C., "The information technology security evaluation criteria," Software Engineering, 1991. Proceedings., 13th International Conference on , vol., no., pp.306-312, 13-16 May 1991.

[4] The Common Criteria Portal, at http://www.commoncriteriaportal.org.

[5] Hunstad, A.; Hallberg, J.; Andersson, R. , "Measuring IT security - a method based on common criteria's security functional requirements," Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC , vol., no., pp. 226- 233, 10-11 June 2004.

[6] Shapiro, J.S., "Understanding the Windows EAL4 evaluation," Computer , vol.36, no.2, pp. 103- 105, Feb 2003.

[7] J Hearn, ”Does Common Criteria paradigm have a future?”, in IEEE Security & Privacy, vol 2, no.1, 2004.

[8] Prof. Kenneth N. Waltz's Political Realism Wins James Madison Lifetime Achievement Award at http://www.columbia.edu/cu/pr/ 00/03/kennethWaltz.html

[9] Hayden, Michael V., “The Future of Things Cyber”, Strategic Studies Quarterly, Spring 2011.

[10] Sterner, Eric, “Retaliatory Deterrence in Cyberspace”, Strategic Studies Quarterly, Spring 2011.

[11] The Common Criteria Portal, Laboratories, at http://www.commoncriteriaportal.org/labs/

[12] Communications-Electronics Security Group (CESG), UK Government, at http://www.cesg.gov.uk/find_a/cert_products/index.php