Is the Common Criteria the only way?

By Dr. David Brewer, Gamma Secure Systems Limited

Working with many product vendors and other users of evaluation criteria, since their very conception in the days of the Orange Book and its European equivalents, sheds light on why the Common Criteria (CC) does some things rather well and others not. There can be no doubt, for example, that the CC has helped some vendors improve their software engineering processes and gain market penetration. On the other hand there have always been complaints about the time and cost of evaluations, technical deficiencies, particularly in the area of "evaluation by parts", mutual recognition and so on.

It is interesting to compare these experiences with developments in other areas of information security over the same time frame, such as computer audit as seen from the perspective of the accountancy profession. In doing so, we learn that different groups of experts have tackled similar problems but in widely different ways.

This paper examines the history of the CC and its predecessors, in comparison with other standards, such as information security management and computer audit. It identifies their strengths and weaknesses and suggests some ways that the CC community could learn from techniques used in other areas of information security in the future.

History

The CC and its predecessors

Prior to 1985, UK pioneers were performing IT system evaluations both for government and for commercial enterprises, such as banks, without the hindrance of published criteria. Often as not, there was no system documentation. Their job was to find security flaws and they did this using all manner of sophisticated analysis and testing techniques, including penetration testing and formal code analysis, and were able to express their results in a form that the business manager could understand [1].

The "Orange Book" [2] was published by the US DoD in 1985. Set against the backdrop of a mid 1970's computer paradigm, it is a specification for operating systems to meet US policy for confidentiality in the context of the Cold War threat.

Splendid as it was, for it combined assurance with functionality for a range of threats, it was not directly relevant to the UK, as UK policies were different and the authorities were more interested in the security of systems, not products (which incidentally should suggest that we should not be interested in composition, as it is a decomposition problem – you start with the system requirements and decompose that to individual component requirements, not start with products and work out what sort of system you might build.)

Despite this, the UK Department of Trade and Industry decided that product evaluation was a good idea since it was difficult for non-US companies to have their products evaluated in the US, and so after not much ado the ITSEC [3] was created, along with a set of commercial evaluation facilities.

For commercial reasons, the ITSEC split functionality from assurance, and established a framework of "cook book" criteria since in order to mass-produce the facilities we had to rely on staff with significantly less experience to carry out the evaluation work. For political reasons the EALs were aligned with the US definitions.

A particular mistake was to assume the waterfall model, or more particularly that vendors could describe what they did in terms of it even if their established practices were different.

Nevertheless, the publication of the ITSEC was a watershed. The US community started talking about "Fortress Europe". The US vendors responded by bringing their products to Europe for evaluation, the US government by producing the Federal Criteria [4] to demonstrate that the Orange Book was still OK.

The Canadians, with strong links to the US and to the British, stood their ground and developed their own criteria [5], in which they proposed a catalogue of security functionality.

And with that was set the scene for a glorious compromise: the CC – the best of the US, Canadian and European approaches, and, as its legacy, the failure of all of them to address the commercial realities of the market they would be getting into. Is not hindsight a wonderful thing!

Vendor and User Experiences

Some vendors found conformance to the CC a benefit in improving their software engineering practices.

There should be no doubt of this, but this is not the purpose of the CC – that is the role of standards such as ISO 9001 [6].

There was a sudden take-up of the ITSEC in the mid 1990s. It was as if lots of CEOs and CFOs suddenly woke up to the fact that if their product was not evaluated then they would loose market share. Previously, no competitor had an evaluated product so it did not matter.

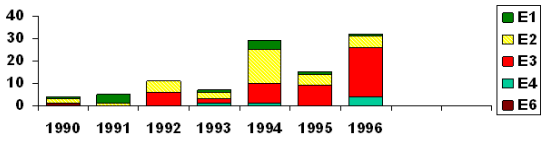

Figure 1: Take-up of ITSEC

To illustrate the significance of this, one US vendor took advantage of UK procurement rules, which stated that all firewalls must be ITSEC E4 evaluated and if there were none, then a product in evaluation would be acceptable. This vendor's product was the first firewall to enter evaluation in the UK and so, being in a list of one, was the only product that UK government could buy. Once its competitors realised what was going on and put their products in for evaluation, that vendor's product was certified, and again was in a list of one. That gave the vendor a 2.5 year start – and Cyberguard was thus born!

But as well as successes, there have also been problems:

- There have always been complaints about the time and cost of evaluations. The root cause is the cook book approach of the CC instigated by the lack of experienced staff to carry to security evaluations at the time the ITSEC was written.

- The smart card community, particularly the Smart Card Security Users' Group was attracted by the mutual recognition concept of "evaluate once, approve everywhere", but it did not work. Reasons have been given as the inapplicability of the waterfall model, and the assumption by everyone outside the evaluation community that those in it had sufficient experience and the ability to think laterally in order to understand the "new" smart card development paradigm. Clearly not the case.

- APIs and composition – there have been papers on these subjects describing approaches used by the smart card community at this conference in 2001 (Visa) [7], 2002 (the Taiwanese) [8] and 2003/4 GlobalPlatform [9], but the CC authors have yet to take up the ideas.

- And finally, comprehensibility – how does it relate to the real world of managing business risks?

Information Security Management

Regarding other approaches, consider BS 7799-2 [10], which is a specification for an Information Security Management System (ISMS). It is shortly to be upgraded to the status of a full International Standard, and published as ISO/IEC 27001. The standard starts with the proposition that the world is not static and uses the Deming "Plan-Do-Check-Act" cycle to deal with it. It is a management standard. It instructs people what to do to manage their information security needs covering organisation, physical, environmental, personnel issues as well as IT issues.

Some IT systems never complete evaluation. In these cases, security depends on physical controls and good security management. Trust comes from the ISMS, so if you want to certify anything, certify that.

Accountancy

The accountancy world starts with the proposition that you cannot prevent mistakes and fraud, so have controls to detect them. That has been the case since the Babylonians and their tally sticks. Substantive audit techniques are used, not conformance with this or that standard, although to be fair, there are checklists for weighing up the pros and cons of financial software packages.

Commonality and Differences

All three approaches, the CC, ISMS and accountancy are concerned with information security but:

- The CC concerns IT. Its focus is on "*preventing* the event", and uses cookbook evaluation criteria.

- Accountancy (computer audit) focuses on "*detecting* the event", and uses substantive audit techniques.

- ISMS focuses on business management and the dynamics of real world situations.

Conclusions and Lessons the CC could Learn

Our first conclusion is that there are many different approaches to information security. They all shed

light on the same real world problem but from a different perspective.

Can the CC community learn from this? Well it might if people listened and were prepared, for example, to revisit early assumptions such as evaluator skills. The world has changed. Nowadays there are Masters courses on information security. Royal Holloway (part of the University of London), for example, produces over 100 such post graduates per year.

Rather than emulate other standards in the CC, for example those to do with quality assurance, we should perhaps refer to them or offer choices, e.g. such and such criteria do not apply if you have ISO 9001 certification. So here we advocate some recognition of other standards.

Perhaps there should be a return to the core business of evaluation ,which is the discovery of flaws, and mountains of documentation are not necessary to do that.

But where do you start? At the Fourth ICCC, which was held in Stockholm in September 2003, there was a track devoted to comparing the CC approach with that of information security management. In conclusion, after all the debates had been heard, it was agreed by those present to maintain separation between the CC and the ISMS standard but to use them in concert. A major step forward, by the Japanese, has been to identify the bits in ISO/IEC 17799 that assist in defining system evaluation requirements. The next step would be to identify those bits in ISO/IEC 27001 that duplicate what is in the CC, and perhaps initially at a national level (because if it works, other nations will follow) offer alternatives, i.e. if you have ISO 9001, 27001 etc, this and that CC criteria are deemed to have been complied with.

Then, perhaps again at a national level, we could address problems such as API and composition using the ideas pioneered by Visa [7] and GlobalPlatform [9]. Bring in SFRs to deal with detection [9], and there is a way ahead.

References

[1] "*EFT-Evaluation: A craftsman-led approach*", Brewer, D.F.C., 1986, www.gammassl.co.uk/topics/hot3.html

[2] "*Trusted Computer Systems Evaluation Criteria*", US DoD 5200.28-STD, December 1985, familiarly known as the "*Orange Book*"

[3] "*Information Technology Security Evaluation Criteria (ITSEC)*", Version 1.2, Office for Official Publications of the European Communities, June 1991

[4] "*Federal Criteria for Information Technology Security*", Draft Version 1.0, (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993

[5] "*Canadian Trusted Computer Product Evaluation Criteria*", Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993

[6] "*Quality management systems – Requirements*", BS EN ISO 9001:2000

[7] "*The Open Platform Protection Profile*", Kekicheff, M., *et al*, Proceedings of the Second International Common Criteria Conference, Brighton, UK, 2001(available from http://www.gammassl.co.uk/topics/OP3-ICCC2.html)

[8] "*Proving Protection Profile Compliance for the CCL/ITRI Visa Open Platform Smart Card*", Wang, C., *et al*, Proceedings of the Third International Common Criteria Conference, Ottawa, Canada, 2002(available from http://www.gammassl.co.uk/topics/smart%20cards/iccc3.html)

[9] "Dealing with smart cards as evaluated systems", Kekicheff, M., *et al*, Proceedings of the Fourth International Common Criteria Conference, Stockholm, Sweden, 2003 (available from www.gammassl.co.uk/topics/smart cards/iccc4.html)

[10] "*Information security management systems - Specification with guidance for use*", BS 7799-2:2002, British Standards Institution