Steven J. Murdoch
University of Cambridge
Computer Laboratory
15 JJ Thomson Avenue
Cambridge
CB3 0FD
United Kingdom

Dear Stephen,

Thank you for providing us with an early copy of your report [DRAFT]. In this paper you raise a number of points, both in respect of the two particular devices that you examined, and in respect of the Common Criteria (CC) certification process. We must immediately point out, however that, by linking the two subjects within the paper, you will mislead the reader since neither of the two devices was actually certified by a Common Criteria Certification Body (CB) and this is not made clear. We request that you make this clear in the paper.

To explain, an important distinction must be made between the terms evaluation and certification . The Common Criteria and their associated evaluation methodology are publicly available international standards (both under ISO and the Common Criteria Recognition Arrangement (CCRA)). They can therefore be used by anyone to guide their own evaluation of a product. The results of such an evaluation however would have no automatic standing with any organisation other than that which performed/commissioned the work. Where certification does take place then the Certification Body ensures that the process has been correctly followed, that the security target is valid, and that the appropriate vulnerability testing has taken place. Only certified products are placed on the certified products list held on the CCRA website at (www.commoncriteriaportal.org).

In the case of the devices that you discuss in your paper these devices have not been certified, and so the UK CB has no knowledge of the devices concerned. You will therefore need to discuss these directly with APACS and/or the manufacturers.

In terms of your general evaluation/certification points however we provide some comments below, which we hope will be helpful as you produce the final version of the paper.

These are listed in the order that they arise in your paper:-

Common Criteria implicitly assumes a waterfall model (p.11) It is certainly true that the current version of CC (Version 3) fits most easily with a waterfall model of development but there are a number of evaluations where this has been adapted to other, more evolutionary approaches. A number of open source products have been evaluated and certified for example. Furthermore, as described below, the CC development board is currently considering a range of evaluation approaches that could further increase the flexibility of the criteria and their application to a wide range of development processes.

Proliferation of Protection Profiles (p 13) The paper observes that there are a number of protection profiles, but fails to point out that these only become relevant when they are referenced by a security target. In effect they simply shorten, and improve the clarity of security targets. As far as we are aware, the example used in the paper (the ATM PP), has not been used in any security target and hence has no connection to any certified product. When approving a security target for any such evaluation, one role that a certification body would perform would be to require that aspects of the product, such as the security policy that it was intended to enforce, would be sufficiently well defined for the evaluation to proceed. Therefore your observation would not, in practice, hold for a certified product.

Economics of the security evaluation process (p 14) Clearly, without external control, it is possible for market competition to cause a 'race to the bottom' as the paper describes it. However this is precisely the reason why Certification bodies and other regulatory bodies are involved in the overall quality control. In this regard it is worth noting that the UK Common Criteria laboratories also have to be approved to ISO 17025 by the UK's national Accreditation Service UKAS. The UKAS assessment provides a regular overall audit (and also, incidentally, regularly audits the CB itself against the international standard for certification bodies EN45011). The CB then has a direct involvement in maintaining the quality of each of the individual evaluations for certification. These mechanisms counter any tendency for such a 'race to the bottom'.

Furthermore, the statement in the paper suggesting that 'agencies appear never to have de-approved a licensed lab for fear of undermining confidence' provides no evidence at all for the existence of such a fear. In fact the CBs involved in the international CC recognition arrangement each ensure that their labs fully meet the CCRA requirements and use a variety of techniques to do so. Removing a licence would be the last resort. Your observation that no lab has been explicitly 'de-approved' can equally well be used to demonstrate the efficacy of these more elegant approaches.

Vendors are indeed, as is observed, able to take their products to any of the evaluation laboratories but, again, there is only one CB in the UK and the CB operates across all UK labs to ensure that a consistent quality is maintained. There are then a number of mechanisms (such as regular dialogue between scheme directors and regular assessment by other schemes), which are in place to promote consistency between schemes internationally.

Relevant developments taking place in UK Information Assurance and in the wider Common Criteria development cycle.

Following an assurance workshop/brainstorm that a representative of your institution took part in and contributed to, the UK has been pursuing a number of innovations in its assurance approaches. Amongst the more fundamental being the increased utilisation of evidence based assurance (flexibility in evidence chains), a whole lifecycle approach (increased consideration of operational assurance, including flaw remediation processes, etc.) and approaches that move away from certificates and towards detailed reports describing residual risks etc. Some of this, together with lessons learned from a joint UK/US trial application of the approaches, was briefed at the International Common Criteria conference last year. These and a number of other areas of improvement are now being considered by the Common Criteria Development Board for inclusion in the next version of the criteria (or immediate operation within schemes where no changes to

criteria are needed).

Within the UK we are planning to hold a further assurance workshop (focussed on the academic element) and would be very pleased if you would attend or be represented at that. In the meantime we are also happy to meet/correspond to discuss the background to Common Criteria and UK assurance in general.

Finally, of direct relevance to your initial report, is the formation of a European based sub-group to address the particular needs of the evaluation methodology for card payment terminals. The draft press release for this initiative is attached (please treat as a draft it may change). Since the CC and CEM are written to provide the overall security and evaluation requirements across a whole range of IT products we have found, over a number of years, that for specialised devices such as Smartcards there is a need for specific guidance regarding how these must be evaluated. The specific evaluation requirements are developed by a group of evaluation laboratories, manufacturers, and government personnel and, once agreed by the CCDB and the CCMC (CC Management Committee), are issued as mandatory supporting documents (they must be applied for mutual recognition to hold). Examples of these for Smartcard evaluation can be found on the CC website (www.commoncriteriaportal.org). Behind each of these is a significant amount of development and collaboration work. The intention of the JTEMS group is to provide the same level of collaboration, guidance, and evaluation requirements for Pin Entry Devices etc.

Yours Sincerely,

David Martin

Technical Director for Assurance Services CESG and UK Common Criteria Scheme Director

References

[DRAFT] Thinking inside the Box: System-level Failures of Tamper Proofing (Anderson,R; Drimer,S ; Murdoch,S) downloaded fromwww.cl.cam.ac.uk/users/sjm217/volatile/ccpedtest.pdf December 2007