File 20100329.0936: Leftover bits from the paper I just finished writing in an all-nighter:

When are criteria unstable?

every time a major revision is made to the

times when it occurs: CC introduction, CC revisions, DCID 6/3 to NIST SP 800-53 transition

times when it does not occur: when the developer chooses not to submit for re-evaluation under the new criteria; when installed systems are not re-tested; when systems already in development under ongoing contracts are 'grandfathered in' under the old rules.

Notes:

This research aims to streamline the certification and accreditation (C&A) of security features for existing IT systems, particularly in those cases where a new or changed C&A programme imposes new requirements on a system that is already known to function acceptably well in field deployment.

This is practical research with wide applicability to security-critical systems in the classified/government sector. It is believed likely that the same thing will become important to commercial users in future, beginning with health care and financial services as the result of new regulation.

1 Thesis

The plan of attack is three-fold: firstly, to take advantage of an unparallelled opportunity for a case study in which a complete set of project records—emails, schedules, plans, reports, draft documents, and diaries—from a recent CC evaluation have been made available for study. Secondly, to develop an open methodology (with tool support) for performing successful CC evaluations on existing IT systems. Thirdly, to validate the new methodology on a bespoke government contract software development project under realistic conditions and publish the results to the software engineering community.

2 Summary

This is a practical problem leading to a solution to the need for effective and low-cost security C&A. Further, it begins by taking the difficult step of publishing details of a large case study that was not successful.

Science and engineering learn from failures, but they can only do so if the results are studied and published. Indeed, the experience of the case study described here cannot be just an isolated aberration; it is well known that C&A is overly expensive and time-consuming for the benefit received, but published case studies—especially unsuccessful ones—are so rare as to be virtually nonexistent.

References