File 20080509.1117: Weekly activity report 0032:

weekly activity report 32 (loughry)
Robert Loughry [robert.loughry@stx.ox.ac.uk]
Sent: 09 May 2008 11:17
To: Andrew Martin [sabbatical@andrewmartin.name]; Joanna Ashbourn; Niki Trigoni
Cc: robert.loughry@stx.ox.ac.uk
Attachments:
Weekly activity report no. 20080509.1036 sequence no. 0032 week 3 TT

I met with Dr Martin after Reading Group on Wednesday, showed off the current iteration of thesis problem statement.

Thesis:

The way that IT security evaluations of existing systems are done today is all wrong. This applies not just to the Common Criteria, but to U.S. DoD and IC C&A processes in general: (DODIIS, DITSCAP/DIACAP, SABI/TSABI, CDMO, and so forth). The current way things are done, starting with an ST honestly describing the TOE with all its warts, is a recipe for delay in the validation process and disaster in evaluation. The way to make the process work is to write an evaluatable ST first, and then transform that into an HLD/LLD/security-policy/correspondence-model to match the ST without over-promising.

Outline of the draft Transfer Report:

I. Introduction and history of the case study (motivation)

II. Literature survey

III. Methodology

A. The results of doing it wrong (anonymised case study)

i. Ground rules, including interviews, anonymisation, handling of proprietary and classified information, and university research review board approvals that will be required.

B. Plan for doing it right (theoretical component)

i. Example of using the Single Transformable Description (SXD) to encode a validatable ST and to show step-by-step how it can be transformed into artefacts.

C. Research sources

i. C&A standards documents

ii. CC-CMTS archive

iii. Project records and participant interviews

iv. The literature

D. Research methods

IV. Research Plan

A. Cost, schedule, deliverables, criteria, plan

NOTES: I have dug up a few old transfer reports from previous years to use as a model, but haven't got read them yet. So sections of the outline likely will move around a bit. The intent, however, is to be able to present a solid work plan for the next year, describing exactly what work needs to be accomplished, what the success criteria are, estimated schedule, and---especially---where the weak spots are in the methodology and plan.

--
Joe Loughry
DPhil PRS, Computing Laboratory
St Cross College, Oxford

End of WAR 0032.

References