File 20110401.0306: Weekly activity report 0182:

weekly activity report 182 (loughry)
Joe Loughry
Sent: 01 April 2011 03:06
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org;
chip.auten@comcast.net; edloughry@aol.com; diane@dldrncs.com;
Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com

Weekly activity report no. 20110331.1901 (GMT-7) sequence no. 0182, week 8+3 HT

In attempting to explain the current state of C&A practice, I had to go back this week to the standards for DIACAP (DoDI 8510.01) and its predecessor, DITSCAP (5200.40) and re-think them using current information. I watched a very interesting presentation this week from Steve Welke of Raytheon TCS in which he made the assertion that Assessment and Authorisation (A&A), in the mould of the NIST interpretation rooted in SP 800-39 is finally gaining traction in both the SABI and TSABI worlds (modified in the latter case by CNSS). The term ‘C&A’, he said, ‘...implies a finality that led people in the past to try to pick up an accredited system and put it down some place else.’ A&A, conversely, correctly reflects a security authorisation process. I am trying to get hold of the author of that presentation so I can cite him properly. Without a doubt, the R’’ case study was the first to apply the NIST approach in the wake of ICD 503.

I found the treatment of scientific hypotheses in phenomenological research discussed in an old book chapter by Dalton (1959) highly useful this week; for research inside organisations, that author gives good advice on writing up results. I am lagging my schedule for Chapters 1--4 but confident of getting them done in time to submit for COS; fewer distractions and more time to work this week are helping tremendously. For Lockheed, I wrote a contribution on SSD forensics for a capture manager this week that was inspired by Wei, et al.’s research but extended in the direction of improved SSD design for forensics-friendly and emergency-sanitisation--facilitating uses. In the context of 8570.01-M training for DAAs, I read the newly issued DoD 3305.13, dated 14th March, which is relevant to the NIST SP 800-137 continuous monitoring policy in the context of C&A for NSS.

Status: writing Ch.˜2 and thinking about Ch.˜3 for COS application in April. I will send a chapter to Dr Martin as soon as I have something written that I am willing to release.

Joe Loughry
Doctoral student in the Computing Laboratory,
St Cross College, Oxford

End of WAR 0182.

References