File 20100514.0747: Weekly activity report 0136:

weekly activity report 136 (loughry)
Joe Loughry
Sent: 14 May 2010 07:47
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; andrea@hpwtdogmom.org; chip.w.auten@lmco.com; diane@dldrncs.com; Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com
Attachments:
Weekly activity report no. 20100513.1125 (GMT-7) sequence no. 0136, week 3 TT

My paper submission to the Unified Cross Domain Management Office (UCDMO) conference was rejected. The email from the conference organiser (NSA) merely said that all tracks have been filled. I think they were probably looking for more product-oriented presentations than theoretical papers. I am turning it around immediately and submitting next to the 2nd ACM Workshop on Assurable and Usable Security Configuration (SafeConfig), to be held in Chicago in October. The ACM Special Interest Group for Security, Audit and Control (SIGSAC) that runs this workshop is a better fit for the paper's topic anyway. I tried to register an abstract today but the conference web site is having problems. As I described in report 134, I believe this conference would be interested in the general problem of setting security configuration parameters on a CDS that reflect risk mitigations required by DAAs at different security levels. It is like a microcosm of their problem (that of setting security configuration parameters consistently across large collections of security appliances in a network) in one box. Abstract registration for the workshop is 7th June; submissions are due 28th June. I need to add to the following abstract a new introductory sentence or two explaining what a CDS is for an audience that might not be familiar with the terminology. The rest of the abstract should be nearly ready to go tomorrow, or as soon as they get their web site fixed. Before submitting a new abstract I will update the PIRA system at Lockheed for review for public release and start a new case number for the ACM workshop.

Title: Information Asymmetry in Cross Domain Accreditation

Abstract: The theoretical difficulty of cross domain systems emerges from the fact that by definition they span at least one boundary between security domains controlled by different data owners. Consequently, new installations of certified solutions regularly encounter security testing criteria that represent the duplicated responsibility for residual risk of multiple data owners. Each data owner perceives a different set of risks A that would be desirable to mitigate, a set of risks B it is possible to mitigate, and their relative complement $A - B$, being the set of residual risks acceptable not to mitigate. Time and cost inefficiency in multilateral cross domain system accreditation to this point arises necessarily from asymmetry of knowledge, but there is room for a solution: the developer or installer of a cross domain system may know about extant risk mitigations that not all data owners are cleared for. If it were possible securely to establish amongst data owners a concord about the true extent of residual risk resulting from overlapping risk mitigations and testing, the unnecessary cost of duplicated effort could be greatly reduced. In support of this goal, a new tool, called {\it nihil obstat}, is being developed to present accreditation data in a common format.

I did not meet with Dr Martin this week because he is teaching a class. Updates to my paper on 'Certification to Unstable Criteria' to respond to reviewer comments are due to the conference organiser in a week. I will present the final version of that paper to the Security Reading Group on Wednesday 19th May. Also on the same day I will be giving a talk about TEMPEST to the Secure Coding reading group at Lockheed Martin at lunch time via multicast.

Regarding the RM 5.0 certification case study, I attended another classified telecon amongst the certifier, test labs, programme office (government sponsor) and software developer today. Without going into details, the interaction between the NSA penetration testing laboratory, IV&V contractors, programme office and developer continue to yield fascinating information about how the CT&E process actually works---in contrast to how it is described in the standards documents. There is a complex multi-way disagreement over some issues, which should be resolved in a few days after Charleston's official report is received. The installation and testing schedule for Beta 2 will slip one week to the right. It is not known whether that will change the estimated date (20th August 2010) when certification and approval to field the new system are expected to occur.

Travel reservations have been confirmed for the VALID 2010 conference in August. My college may have up to 200 to help defray travel expenses for presenting at a conference; I will apply to the Bursar for that and also check with the department to see if they have any.

I am concentrating now on finishing the camera-ready paper for one conference, abstract and draft paper for another conference, and the outline of a new journal article. Before my next meeting with Dr Martin (probably Thursday of next week), I want to have all those things done.

Current list of tasks in priority order, most urgent priority first:

Immediately:

1. Camera-ready copy for VALID 2010 addressing reviewer comments in time for Reading Group on Wednesday and conference deadline next Friday.
2. Register abstract for ACM workshop (web site problems prevented doing it today). 3. Prepare two talks for Security Reading Group and Secure Coding group (Lockheed Martin) on 19th May. 4.Go through final presentations from RMUG for names, dates, addresses, and data relevant to thesis. 5. Finish list of email addresses for practitioner survey, participant survey, and user survey; develop questions, enter in SurveyMonkey and test. This is very late; goal is now 25th May.
6. Re-outline the Crosstalk journal paper based on what was learnt in RMUG and 5.0 CT&E Beta 1 IV&V and pen testing; extend the outline; write draft paper; plan to submit to journal by 30th May. 7. Outline new ACM workshop paper; begin writing. 8. Extend the outline of the methodology chapter.

As soon as possible:

9. Update dissertation Table of Contents. 10. For Chapter 3 or 4, start writing interpretation of first case study results and second case study preliminary results. (This will be needed for confirmation of status.)
11. Begin writing progress report for confirmation of status. 12. Fill out paperwork for UK student visa extension for June deadline. 13. Update the schedule. 14. Design of accreditor information coordination tool based on feedback from first three papers. 15. Apply for confirmation of status---I want to submit the forms with written work by end of June for August or September.

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

End of WAR 0136.

References