File 20100430.0040: Weekly activity report 0134:

weekly activity report 134 (loughry)
Joe Loughry
Sent: 30 April 2010 00:40
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
Attachments:
Weekly activity report no. 20100429.1449 (GMT-7) sequence no. 0134, week 1 TT

No meeting with Dr Martin this week because of Info Security Europe.
I have been in meetings all week between the U.S. Navy Programme Office
(the second case study project's government sponsor), the developer,
and with various users of the system.

Comments and presentations this week from users of the Radiant Mercury
system have enabled insight into the C&A process from the perspective of
CDS users. The developer expects to receive the Beta 1 test report from
IV&V tomorrow. Presentations all week from the developer, programme
office, and users have highlighted the extreme need for version 5.0
of the software to be certified and deployed as soon as possible.
The developer continues to be severely underfunded, although it is
not entirely clear to me whether this is the fault of the programme
office or another agency further upstream. The programme office COTR
was sitting right next to the developer's programme manager when the
latter described the excruciatingly tight funding situation in front of
an audience of users, and even after watching the exchange I still do
not understand the exact relationship there. I plan to sit down with
the programme manager and ask him to explain it. I am sure he will be
willing to do so, whenever I can catch him at a good time.

NSA I173 has a new model for Cross Domain CT&E called the Risk Decision
Authority Criteria (RDAC). It assigns a scale of five rating levels to
three types of risk: Technical Risk (TR), Data Risk (DR), and Attack Risk
(AR). For example, DR is assessed for risk of spillage or policy bypass
threat as Low, Medium, High, Extreme, or Unlimited. For each combination
there is presumably a matrix specifying which risk mitigations are thereby
required. It sounds like this model is being floated as a possible
future methodology for CDMOs to harmonise their evaluation criteria.
I do not think it has the force of policy within UCDMO yet.

There is a Classified Connection Approval Office (CCAO) that I have been
hearing mention of lately. I do not know what this is yet but I will
find out. It seems to be in DOD, not IC.

I have been working on the UCDMO conference paper. Notification for the
other conference in France should arrive tomorrow. I need to work on
the Crosstalk journal paper; that is behind schedule. The unexpectedly
large number of users who descended on the developer facility this week
wanting to talk about their accreditation experience (among other things)
took up almost all my time. I collected scores of new artefacts and
took extensive notes on reported issues. Even with all that new data,
at the end of the week I feel more confused than ever. As a way of
overcoming the feeling, I intend to work on a paper this weekend.

Surveys are still not done. In my defence, I spent half the week
listening to users, developers, and government certifiers talk about
closely related topics. The new information will improve the survey
questions, and I gathered some new names of people to add to the survey
population.

My talk on emissions security (TEMPEST) is postponed to 19th May because several attendees must attend a conference in Washington, D.C. next week.

Experience with the new Lockheed automated tool for review for public release has been mixed. The tool does not seem to understand the difference between a closed NSA conference and an open conference in France where people from different countries will naturally be present. The system seems to overreact automatically and flag every submission for Directorate of Freedom of Information Security Review (DFISR) when it is clearly not applicable to any of the FOIA exemptions in 5 U.S.C. Section 552(b)(1) through (b)(9), summarised as:

(b)(1) classified national security information; (b)(2) internal agency personnel rules and practices; (b)(3) records specifically protected by another law; (b)(4) trade secrets obtained from a private source; (b)(5) internal agency deliberative records; (b)(6) personal privacy; (b)(7) law enforcement investigatory records; (b)(8) regulation of financial institutions; (b)(9) geological and geophysical information.

I received a CFP this week for the ACM Workshop on Assurable & Usable Security Configuration (SafeConfig) to be held in Chicago, Illinois in October. The workshop is about setting security configuration parameters consistently across large collections of security appliances in a network. I think the workshop might be interested in the problem of setting security configuration parameters on a CDS that correspond to risk mitigations required by DAAs at different security levels. It is like a microcosm of their problem in one box. Abstracts are due 7th June; submissions are due 28th June; notification is 6th August. Thinking about it as a model of the enterprise security configuration problem, I have some ideas for a paper. I will put them in an outline for our next meeting.

My next meeting with Dr Martin is scheduled for Thursday, 6th May 2010 at 1400 Oxford time.

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

1. Review all presentations captured this week for relevant information, names, addresses, and data relevant to thesis.

2. Re-outline the Crosstalk journal paper based on what was learnt this week. Extend the outline. Write draft paper. Submit to journal by 14th May.

3. Finish list of email addresses for practitioner survey, participant survey, and user survey; develop questions, enter in SurveyMonkey and test. Goal is now 7th May.

4. Begin outline for new ACM conference paper. Write abstract.

5. Extend the outline of the methodology chapter.

6. Write the rest of the UCDMO conference paper.

7. Update dissertation Table of Contents.

8. For Chapter 3 or 4, start writing interpretation of first case study results. (This will be needed for confirmation of status.)

9. Begin writing progress report for confirmation of status.

10. Fill out paperwork for UK student visa extension in April for June deadline.

11. Update the schedule.

12. Apply for confirmation of status---I want to submit the forms with written work in June for August or September.

13. Development of accreditor information coordination tool.

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

End of WAR 0134.

References