File 20100521.0525: Weekly activity report 0137:

weekly activity report 137 (loughry)
Joe Loughry
Sent: 21 May 2010 05:25
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. 20100520.1912 (GMT-7) sequence no. 0137, week 4 TT

I presented my VALID 2010 paper to the Security Reading Group on Wednesday. John and Cornelius were there. I wrote this short paper for the purpose of introducing an audience to the background of CDS since there aren't any---or hardly any besides the UCDMO conference---gatherings in my sub-field (there is not a lot of literature either on the subject of security certification and accreditation, besides the standards documents). One problem I keep encountering is that I always have to spend a lot of time explaining background to a new audience, and I am really constrained by the short page limit on this paper. Reading Group on Wednesday more quickly got into the important parts, because the participants had all heard my previous seminars in Oxford and knew the background.

I told them I am working on a related idea that characterises the residual risk accepted by accreditor A which might be different from the residual risk acceptable to accreditor B because whilst both probably agree on the set of threats it is desirable to mitigate, they might have different security clearances, hence know about different sets of risk mitigations which are at least partly disjoint. That is going to be the ACM paper I will finish writing as soon as I get the camera-ready copy for VALID 2010 submitted. It is due to the conference editors by end of day tomorrow.

Tip for giving presentations: don't talk about 'accreditors' before explaining what an 'accreditor' is. The audience probably hasn't read your paper yet. The purpose of a conference talk is to make people want to read your paper. A conference talk, especially at a conference like this where the audience probably is not familiar with your problem domain at all, should be aimed at a level explaining all specialised terminology the first time it is used. This will not be an audience of specialists in C&A of classified systems; they will be specialists in testing and validation.

John and Cornelius were a great help. Their thoughts on the paper led to a better understanding of what the reviewer comments actually were trying to say. Cornelius said that in Section II, I really have two problems, not one. The paper first talks about ST&E, but then gives two examples of CT&E, and then it is back to talking about ST&E again. That section was unnecessarily confusing. John asked about how I expect it to scale; I talked about reducing the number of rounds of ST&E after a system is CT&E'd from 1000 rounds of (nearly identical) testing down to around 10. Those numbers come from an estimate of total life cycle installations of a typical CDS, including re-certifications and periodic re-accreditation of sites due to environmental changes. I want to have a more persuasive model and estimates of those numbers available by the time of the conference in August, since I expect questions about it.

John asked whether the tool is intended to collate evidence from previous accreditations? Answer: yes. The idea is never to have to run the same test, on the same equipment, with the same connections, by the same people, using the same test procedures more than once.

The accreditors might be different.

Cornelius asked if my problem is still too big. I agree with that concern. The VALID 2010 paper, placed next to the draft of my ACM paper which is really more about a theoretical foundation for the new tool, shows up the difference starkly: you can see the evolution of my thesis from a first case study of one unsuccessful Common Criteria evaluation, through a second case study showing that success is possible, which then suggested an idea explaining how flow of information in the right way leads to success (and the wrong way, to failure) which pointed to the need for a tool, which needed a theoretical foundation to inform its design, which led finally to understanding that there is a neat little mathematical problem at the core of it. Cornelius is right, I may have two different research projects here and it might be time to choose one. I have a limited amount of time to finish. When I go to Confirmation of Status soon, the assessors might look at my preliminary results and tell me to break it up, because they want me to finish in less than a year from that time. I really have two different problems here, and to Cornelius they look nicely separable. I may not want to separate them though, in the interest of making a more significant contribution. Markus Kuhn's dissertation contains two contributions: a new set of TEMPEST limits on RF emanations derived from first principles, and a narrow look at CRT phosphor impulse--decay behaviour in the optical spectrum. What I have here is enough work for the next three calendar years, but only about one year of time. I intend to finish a well-defined contribution, then continue the research post-doctoral, until it's done. There is plenty of room for future work here, probably five years worth.

John and Cornelius advocated that I should choose one or the other: CT&E or ST&E, and focus on that for the DPhil. I started out in this saga focussed on CT&E, but lately the details of my research (and papers) have shifted to ST&E. Certainly ST&E is performed more often, and probably represents a larger proportion of the total spending on CDS in field installations, despite the fact that CT&E is more visible and gets more attention. I need to talk with Dr Martin about this; I have asked for a meeting when he gets back.

John made a suggestion in Reading Group that got me unstuck on the introduction to the paper. He suggests briefly highlighting the similarities between the two examples before talking about the more extensive differences. As it stands, it looks to the reader like two completely different systems, when in fact they are the same software. This illuminates something that one of the reviewers said in comments from the conference committee. I know how to fix it now. Also, how is CT&E similar to ST&E?

There is still a problem with the submission system at the ACM conference (SafeConfig). I emailed the editor but have not received a response yet.

The Prime Minister cancelled the UK ID card project, which changes the student visa process. I got a notification from the International Students Office about a meeting I have to attend.

I gave a talk at Lockheed yesterday to a small audience on the subject of emission security: conducted emanations, RF, optical, acoustic, thermal, induced, and exotic attacks. The talk was well-received and I was asked to repeat it for the multicast on 15th June.

I put a paper on the wiki for next week: 'Experimental Security Analysis of a Modern Automobile' by Koscher, et al. (Oakland, California: IEEE Symposium on Security and Privacy, 16--19 May 2010). On an internal

Lockheed Martin mailing list, I posted a short article called ‘Automobiles are Cross Domain Systems’ in which I made the case that they are that, and manufacturers do not recognise it yet, but the same techniques that are used to interconnect classified networks are applicable to the multiple LANs running in the chassis of your car. The key point of the research by Koscher, et al. is that the particular car they tested was not air-gapped. One component (the telematics ECU) connected to both the low-speed untrusted network and the high-speed safety-critical network and was found not to implement the required authentication as specified in the CANbus standard. So any device on the untrusted network (such as an aftermarket stereo) could re-flash the telematics ECU, add new code to act as a network bridge, and compromise the trusted network. The researchers gained full control of throttle, brakes, door locks, lights, windscreen washer and wipers, and instrument panel displays.

The RM 5.0 CT&E telecon this morning (my second case study) provided a little more insight into what the disagreement between the two camps is all about. The purpose of the meeting was to go over the developer’s final response to the certifier’s reply to the developer’s response to the certifier’s findings, but what really came out was a philosophical difference over the meaning and scope of CT&E in relation to ST&E. There are voting members of the CDTAB (Cross Domain Technical Architecture Board) on both sides of the issue. The certifier wants to remove certain functionality from the CDMO baseline configuration because the certifier feels that it has null functionality. The developer and the Programme Office argue that function is inherent in the framework, that the framework is there for each accreditor to specify how it is to be used at a particular site, and that the choice of what to hang on the framework is the accreditor’s. The certifier is afraid that if the CDMO baseline contains an adaptable framework, some sites will configure it in a stupid way, and the result will be insecure. The developer and the Programme Office counter that because the accreditor formally accepts responsibility for the residual risk and correct operation of a system at a site, no accreditor would allow the framework to be configured that way. I apologise for the vagueness of this description but I cannot go into details and it is the disagreement between developer and certifier that is significant to my thesis. Another thing that came up was the fact that the IC (Intelligence Community) certifiers are ready to proceed but that SABI (Secret and Below Interoperability) certifiers are not. ‘That completely defeats the purpose of the UCDMO’ commented one participant. This is going to be an entire chapter, I can tell.

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

Immediately:

1. Camera-ready copy for VALID 2010 is due tomorrow. 2. Register abstract for ACM workshop (web site problems are still blocking this; editors contacted). 3. Outline for Crosstalk paper. 4. Go through slide packages from RMUG for names, dates, addresses, and data relevant to thesis. 5. Write ACM SafeConfig paper about asymmetry of knowledge amongst accreditors. 6. 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. 7. Talk with Dr Martin about circumscribing the exact contribution I want to claim at Confirmation. 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. Start a new Appendix containing de-anonymisation codes for all participants. This will be a separable appendix. 12. Begin writing progress report for confirmation of status. 13. UK student visa rules have changed; check with International Office. 14. Update the schedule. 15. Design of accreditor information coordination tool based on feedback from first three papers. 16. 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 0137.

References