File 20101119.0254: Weekly activity report 0163:

weekly activity report 163 (loughry)
Joe Loughry
Sent: 19 November 2010 02:54
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org;
chip.w.auten@lmco.com; edloughry@aol.com; diane@dldrncs.com;
Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com

Weekly activity report no. 20101118.1432 (GMT-7) sequence no. 0163, week 6 MT

I have arranged with the assessors Dr Jirotka and Dr Flchais for my
Confirmation of Status viva to take place on Thursday, 16th December
2010 at either 9:00 in the morning or 3:00 in the afternoon. I will
arrive the day before on UA 918 via London Heathrow and remain in Oxford
a few days afterwards to do library research at the Bodleian and in
my college library. I hope to be able to meet with Dr Martin and Dr
Ashbourn in person, as well as taking care of some errands in college
and at the bank. I am so looking forward to being back in my favourite
city again, especially at Christmas.

GSS reports are due next week. I will have my report submitted
before the deadline. The Air Force Research Lab project demanded a
lot of time this week; I ended up logging a lot of hours for Lockheed.
I finished and submitted the yearly progress report to the Air Force
(11,000 words), describing several new results including a few unexpected
ones that suggest a direction we ought to go for new capabilities.
The project is now in Phase III; the report laid out a detailed plan
for development in FY 2011. The project manager is in Rome, New York
this week meeting with the sponsor. I will seriously have to modulate
effort on the probabilistic redaction project carefully over the next
year to avoid adversely affecting progress on my DPhil research.

Because of staying up all night writing that report, I did not get
Simscape installed yet to work on my accreditor model. I contacted
MathWorks and tried to order a single academic research licence
for Simscape, but the web ordering system could not understand that I
already use the University's licence for Simulink, and it tried to charge
me for an additional copy of Simulink, a cost of hundreds of pounds.
The University has no reusable licence for Simscape. I need to talk to
a salesman to get the licence modification I need. I will do that in
the morning. If I have to buy it, I will.

The COMLAB-CS-2010 programme committee met this week to finalise the
conference proceedings and arrange to have them printed. The conference
is tomorrow.

I had a meeting with Dr Martin on Friday to report status and talk about
progress. Dr Flchais told Dr Martin that the written work from my
confirmation of status has gone missing in the University administration
and asked if I could I email a copy of it directly; I have done that.
Dr Flchais also mentioned the possibly of conducting a viva over Skype,
but I am wary of that. Plane tickets to Oxford in early December are
cheap, and I have some errands to run anyway. I would rather go in
person for the viva. Dr Martin is off to Australia at the beginning
of next month; that may be the 7th December event on his calendar.
My viva date at present will not conflict with the IEEE conference;
I am keeping fingers crossed.

I reported to Dr Martin that I am making good progress in several new

areas: talking with Dr Kladko of Aspect Labs in California about CC research, the new case study I discovered (the Advanced Extremely High Frequency, or AEHF project) from 1999 that used a very early version of the Common Criteria---v2.1, and my attempts to get an academic licence for Simscape. I found a price list from Cambridge in early 2010 on the web, but I need to find one that is applicable to reality.

When I was writing an email to Dr Kladko, in the process of trying to write one sentence I realised that the definitions of 'success' and 'failure' in CC evaluations---in fact applicable to all C&A definitions---are more complicated than I thought. I am still trying to work out all the implications of that. It seems I am making good progress; Dr Martin said I sounded upbeat on Friday.

Security Reading Group this week met to discuss the paper by Martin, Davies and Harris titled 'Towards A Framework for Security in eScience'. Attendance was up from the usual number of people. This paper is based on work that Dr Martin did on sabbatical in 2008 on system-level security properties of the work that eScience projects are doing today, seeking a descriptive framework for characterising the security controls---including privacy which is critically important in clinical data---of eScience network collaborations. There is an apparent spectrum, from particle physicists at one end who need few controls on access but are highly concerned with integrity of information, to the other end of the spectrum where clinical researchers constantly need access to personal information. In the middle are engineering projects with safety critical, regulatory, competition-sensitive or forensic requirements, and of course the special case of eScience projects that deal with politically hazardous material, who themselves need to protect against fraud, deliberate manipulation and forensic evidence related to accusations thereof on the data or results. But the spectrum model did not work. They tried thinking instead of a load of criteria, to have different people rate themselves on a catalogue of security controls, indicating whether they need some of this or that. The main contribution of the paper is a set of discrete categories for each aspect. The authors said they were inspired by NIST SP 800-63, which I agree is well designed. Dr Flchais asked for an extension of the work later on, noting that a prescriptive risk analysis would be useful. A synthesis of concepts, descriptive but extensional. Shamal asked where the sample threats came from; Dr Martin replied that they were anecdotally defined, coming from participants in the workshop, who began with domain specialists, then eScience, followed by Trusted Computing folks and finally DRM experts. Shamal related the story he has told us before about using a focus group to gather threats---very context-specific. Are there any non-internet-facing threats that might be specific to eScience? The answer was: not so much levels as bilateral threats. Dr Flchais noted the intriguing progression between levels. In several instances, L2 is qualitatively different from the other levels. I also commented on the similarity to discrete jumps in Common Criteria evaluation assurance levels. Could this be inherent in any levelling system? I wonder.

The kinds of users in an eScience system are different from what you might find almost anywhere else. The most interesting---especially to me, since my research deals with the insider threat explicitly---are represented by the malicious insider and the reverse engineer. The categorisation in the paper is accurate and complete, as far as our group could establish; they are different kinds of users with completely different points of view. Dr Martin cautioned that the levels are carefully not prescriptive, because eScience users are only interested in things that work. For instance, the existence of a level 'zero' in some aspects: L0 represents not doing anything; L1 represents starting to do something. There is,

as the introduction puts it poetically (I thought) an aspirational progression. Everyone in the group hoped by the end of the meeting that this paper turns into a book some day...chapters on what each project did to improve its levels, e.g., from L1 to L3 here, from L0 to L2 there, etc. I thought the only things missing from this paper were a diagram---one would be helpful there---and a set of descriptive scenarios illustrative of typically seen collections of L0-->L4 indications that would suggest a progression that other eScience projects could follow. Harness that aspirational desire!

For next week, I tentatively suggested a paper from Comm. ACM a few years ago on 'Self-Plagiarism in Computer Science'. Not because I thought the paper was any good, however; I think the authors are wrong. This paper, which I found last week, made me angry when I read it. I think the whole idea of self-plagiarism in this field is preposterous, and this paper is deliberately misleading. Look at the development of ideas over the lifetime of a serious researcher: you see a clear progression of of thought from less developed ideas and the beginning of concepts through to a fully thought-out thesis, often many years later in the form of a book or a series of books. Contrast this with what I will call 'temporary experts'---writers who currently are specialists in international finance, but next year they may be writing about polar bears. I hope this paper causes a screaming argument in Reading Group. I really think it is intentionally misleading.

Next week's Security Reading Group might be postponed in favour of a talk being given by Google on warehouse-scale computing Wednesday, if people want to attend that instead. I think it sounds interesting and I would love to hear it, but I will not be in town yet. If the speaker gives out any handouts or a URL for the slides, can someone in the audience save one for me?

I have been looking into the problem of confirmation bias and the advantages of a repeated measures research design over an independent groups research design. Having just learnt about the concept, I of course had to think back to the optical TEMPEST research I did a few years ago, wondering whether it affected the sampling in the research project I did at that time. Regarding the claim in the paper that '30 percent of devices tested were found to exhibit Category III optical emanations' (Loughry and Umphress, 2002a), was there a selection bias? I think that arguably there may have been some, because there was never a randomised sampling of devices tested, but on the other hand the sampling included every LED we could get close enough to measure in an entire computer room, so that was a fair random sampling of all of the devices in a representative facility.

At the RM developer's facility I attended their new Engineering organisation meeting on Thursday. The 5.01 patch is being prepared and tested by the developer now. In addition they are developing a new process for rating maintenance. Under the TCSEC and later the Common Criteria, maintenance of evaluated products based on COTS hardware and operating systems, especially network-facing systems, invariably became an area of contention amongst developers, certifiers, and vendors of the COTS operating systems integrated into evaluated products. The RM developer has seen the problem become only more acute with the increasingly common integration of COTS and FOSS software components into the evaluated baseline as subsystems, e.g., anti-virus, malware scanners, user interface libraries, SSL libraries, LDAP libraries, and database libraries. The issue, in the developer's view, is the TCB boundary. For Rating Maintenance Phase (RMP) reasons, it is strongly in the developer's interest to define any component that the developer depends on

another developer for to be outside the TCB so that asynchronous patches and security updates will not trigger a recertification event. This has been a chronic problem for the RM developer since at least 1998 when the developer first ported the application to an evaluated OS that was actively in RMP at B1 under TCSEC. Around the year 2000, the OS vendor shifted to CC evaluation but was never very good about defining a solid process for reconciling security patches with the evaluated configuration. Consequently, the developer was forced to define its own process and solicit approval from numerous (at the time) U.S. government agencies in order to maintain its certification and accreditation---completely separate from the certification status of the OS, another thing that was absolutely necessary for NSTISSP No. 11 compliance and the only reason anyone ever gives these days for seeking CC evaluation. The solution never was completely satisfactory, but was tolerated implicitly by a series of programme office sponsors and by NSA because all were aware that no superior solution was forthcoming at the time.

The interesting thing this week is that the RM developer is proposing a new solution. The 'OSP' patch concept will separate FOSS and COTS patches and security updates for the first time into a regular outside-the-TCB patch cycle independent of application-level TCB changes, run on a regular schedule that accommodates COTS and FOSS vendor/developer patch cycles. The OSP rate of change will be independent of TCB patches and itself is divided into several categories, each with its own independent and displayed version number. The developer is proposing this solution to the problem of keeping COTS and FOSS components---to include OS security updates, patches, and hardware firmware updates---including non-security-critical OS components to the certifiers in the course of the RM 5.0 SABI deliberations of the CDTAB and DSAWG. This is an important development and represents in my view a significant advance over the previous mode of operation of CDS developers. It shows a recognition by the developer, and presumably the programme office, of how the world actually works as opposed to how standards say it should work. It is unclear whether the OSP proposal was initiated at the behest of the developer's engineering organisation, IV&V, the certification authority or the programme office but the document is now travelling in the direction from the developer to the programme office. The new process, if approved, will allow the developer to respond more quickly to IAVAs and will improve compliance, something that is monitored by agencies other than the programme office sponsor, certification authority, accrediting authorities and data owners.

I obtained a look at the developer's roadmap for post-5.0 CDS improvement, and noted that the planned progression of versions 5.01 through to 5.02, 5.1, 5.2 and 6.0 closely matches the programme office sponsor's COTR presentation to agency management of a sequence of 5.1, 5.2 and 6.0 versions. The feature sets agree, not surprising given that they are negotiated between the programme office and developer according to what the engineering organisation believes is technically achievable. The next major revision of the CDS, designated 5.1, will have a completely overhauled HCI although user-visible changes will be minimal. Underneath, the implementation will have completely changed. The roadmap does not indicate recertification trigger points although I have suggested it to the developer as an improvement.

My current task list (in priority order, most urgent first; work on tasks in this order):

0. Get a licence for Simscape that will work with the University's site licence for MATLAB. If that fails, purchase my own copy of MATLAB, Simulink and Simscape.

1. Rework the Crosstalk article according to latest thoughts. In the outline, I have that R-prime was evaluated under CC v3.0, but I recalled recently that there was an earlier version of the system (call it R_0) for the E project that was supposed to be 'evaluatable' under CCv2.3. R-double-prime was certified under DIACAP as the first test case to replace DCID 6/3, but it looks now like DoD and IC will be put together under the tent by UCDMO soon, as soon as they obtain full control of DSAWG.

2. Thinking about what the definition of 'succeed' and 'fail' are in the context of CC evaluation; 'did not complete validation', 'abandoned before the end of validation', 'failed to receive certification', 'abandoned before the end of evaluation' and 'not submitted for evaluation' are all different and significant events.

3. Get a licence for Simscape and use it to modify the MATLAB simulation to do 4 systems in parallel with the same set of fixed points. Implement Prof. Polak's equilibrium acid test and the double alarm clock option model (should be easy to do in Simscape).

4. Background reading: Pennock and Wellman (2004) on uncertainty markets, Levitt and Dubner (2009) on asymmetric information, Bernstein (1996) on risk assessment (on hold), Karp (2009) on research methods.

5. Ping the following people: Paul Ozura [BAH], Dennis Bowden [San Diego], [Patti Spicer, Charles Nightingale, Hal Forsberg at CSC], Dr Kladko [Aspect]. Tell Dr Kladko when I will be on travel.

6. Small tasks: update first case study chart with changes from last conference; draw fault-tree diagrams for R-prime, R-double-prime and S-star; draw up organisation charts for R, R-prime, S-star, R-double-prime, N, L and G; update documentation of the current set of anonymisation codes.

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

End of WAR 0163.

References