File 20100826.2232: Weekly activity report 0151:

weekly activity report 151 (loughry)
Joe Loughry
Sent: 26 August 2010 22:32
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. 20100826.1427 (GMT+1) sequence no. 0151, week 8+10 TT

This week I have been at the VALID 2010 conference in Nice, France. I heard 48 papers (I could not go to all of them; there were four tracks). Those papers that I heard were Bernstein (2010), Ghetiu et al. (2010) Duan et al. (2010), Mohacsi and Wallner (2010), Martins and Guyennet (2010), Trivedi and Balakrishnan (2010), Kominami et al. (2010), Lill et al. (2010), Barnes et al. (2010), Yang et al. (2010), Du et al. (2010), Marceln-Jimnez et al. (2010), Kaindl et al. (2010), Santos (2010), Pereira et al. (2010), Popovic et al. (2010), Hutter and Toegl (2010), Martins et al. (2010), Akgn and aglayan (2010), Takaki et al. (2010), Aboulsamh and Davies (2010), Lavazza (2010), Dini et al. (2010), Bonnecaze and Liardet (2010), Hashimoto et al. (2010b), Ueno et al. (2010), Hashimoto et al. (2010a), Tu and Huang (2010), Hadaytullah et al. (2010), Kruger and Wolhuter (2010), Patel et al. (2010), Rodoplu and Raj (2010), Hilera and Fernndez-Sanz (2010), Schar et al. (2010), Assad et al. (2010), Simonin et al. (2010), Nkwocha et al. (2010), Breu et al. (2010), Hohenstein and Wiese (2010), Ilyas and Kng (2010), Prez-Ortega et al. (2010), Fahad et al. (2010), Guo et al. (2010), Nguyen and Sood (2010), Eskeli and Parviainen (2010), Hadaytullah et al. (2010), Al-Moayed and Hollunder (2010) and Flores et al. (2010). Some especially interesting ones included: a paper that hid information in reserved bits in the PHY and MAC layers of 802.15.4 radios to attack wireless sensor network (WSN) devices\footnote{I think the authors missed a chance to shut down the attack by having authorised nodes set their reserved bits according to a cryptographic key stream; an attacker, setting his reserved bits randomly, would be detected with probability $1-(0.5)^n$ after n frames had been transmitted; I should have brought this up in the question period, but I didn't.}, another on testing environmental monitoring satellite ground stations by simulating the path of a polar-orbiting satellite with a light plane following a carefully calculated flight profile (they did some hairy coordinate transformations, but when they finished, the simulated and measured curves lined up beautifully; I thought it was the best paper at the conference), and another on using multiple loop antennae to set up zones of constructive and destructive interference in the magnetic fields powering an RFID chip connected to a TPM; by preventing the chip from receiving enough power from spoofed terminals to operate, the authors could control which terminals it would talk to. It was like a trusted path combined with a TPM---neat.

Overall, I thought the quality of papers at this conference was high (there were some not-so-good, but not too many). There were lots of PhD students here. Sessions ran twelve hours a day, not counting coffee breaks and lunch. I listened to the keynote but mainly noted things not to do; the keynote talk was not very good. The panel discussion later in the week was much better: Eric Verhulst talked about 'hardware that executes specifications efficiently' (and software that executes requirements). He noted that stack protection in a microcontroller needs only two registers and two comparators, yet none of them have it. The next stage in safety-critical design, beyond completely proven systems, is to be a little heuristic. Mechanical systems tolerate small failures (such as missing a deadline by a single cycle) better than digital systems do. Mechanical systems---because of their continuous nature---vibrate; they bend, they tolerate a small amount of error instead of instantly shutting down. Keith Stobie talked about heuristic oracles and reasonable consistency; identical queries to Google rarely return exactly the same results; they are mostly the same (reasonable consistency) but differ in the noise. It is a characteristic of distributed databases and map-reduce; the longer the convergence time available, the higher will be the precision.

I saw some interesting analytical techniques that I want to try using; in particular, I want to play with a simulation technique (Boids) that looks to be easy to implement in MATLAB. It had better behaviour than a random model in one of the simulations presented. I saw one or two superb examples of how to do case studies well (Nkwocha, 2010), plus another example of maybe how not to do it (Popovic, 2010). I now have a long of old papers from other people’s references that I want to look up.

My talk went reasonably well. It was first thing on Monday morning; I had twenty minutes and had practised my talk to that limit over and over again. In the question-and-answer period afterwards, one person asked me a nasty question about the statistical significance of experiments done in a simulation. This happens to be something that Dr Martin and I have discussed before; in fact, he asked me that exact same question a few months ago---so I had a ready answer. I answered it totally by reflex. I began by observing that controlled experiments in software engineering are problematic because they tend to be expensive (I cited McCue, 1978). I returned to my previous slide and noted that one case study I had just described cost a year and a half of time and five million dollars. I said I might not be able to justify a 95 percent confidence interval (or whatever your favourite P is) with the results obtained from my numerical model, but I can certainly calculate what it turns out to be. I promised to report the value honestly, even if it’s 0.12. The same guy asked the same question in a few other talks, I heard.

Based on questions from the audience, I have a lot of new anonymisation codes to add to the first case study (that crazy Venn diagram). It needs to grow both forward and backward in time. I have a sketch on paper, will update it in Inkscape when I get back.

I met with Dr Martin before I left for Europe. He approved the following paragraph for ATAS describing my research; I gave it to Wendy Adams who sent me back an official letter for the government’s use:

‘Cross Domain Systems (CDS) for handling classified information complicate the security test and evaluation problem because, by definition, they span security boundaries; in the present scheme, this leads to multiplication of cost with no concomitant improvement in security. This research will examine project records from a pair of related CDS certification efforts in the US and UK with the aim of developing a tool based on a generalisable model of inter-accreditor communication in which not all accreditors are cleared to the same or comparable levels. (The model is therefore useful for both intra- and international security accreditations.) Other data will come from interviews with certifiers and accrediting authorities in the intelligence communities of the US and UK governments; MATLAB will be used to develop an equilibrium model based on microeconomic theory and to perform experiments on the equilibrium in silico. The eventual goal of this research is to reduce the time and cost of certification test and evaluation as applied to CDS systems by eliminating unnecessary re-testing of the same or similar security requirements during accreditation by mutually distrustful data owners whose interests align in minimising the residual risk of the CDS.'

As soon as ATAS comes back to me with a certificate, I can mail my passport to the Consulate in Los Angeles for a new visa.

There is an article in Foreign Affairs this month that reveals new information about last year's attack on DoD. It confirms that it was by means of a flash drive containing targeted malware.

There was a meeting today of the RM 5.0 CT&E participants to discuss regression testing results, schedule update, and the next steps. I could not attend but asked a contact who will be there to provide me with information from the meeting. I have not been getting a good response at all from accreditors in the US government to my emailed questions about their work. I received one response yesterday from Dan Nichols, Technical Director of the UCDMO; he basically said no, in a way that suggests I will not get much further with his office. When I get back I need to talk with Mr Ozura again; he was the one who recommended I should contact Mr Nichols and he suggested that Mr Nichols would be a good source. I will try to figure out what went wrong with the contact.

I have been working on my numerical model some more, although I have not had any time to do anything with MATLAB this week. I have been asked to repeat a talk I gave earlier this year about TEMPEST techniques to a group of IA engineers at Lockheed on 23rd September. I sent some comments to Shamal and Cornelius this week about draft papers they asked me to read. Even on weeks when Reading Group doesn't meet, people still send papers around.

When I get back, I want to talk to Dr Martin about confirmation of status.

My current task list (in priority order, most urgent first):

To be done immediately:

1. Type up notes from conference (I will finish tomorrow).
2. ACSAC submission deadline is in two weeks. I want to get the most recently rejected paper revised and submitted to this conference.
3. Ping Mr Ozura again regarding Dan Nichols' refusal to contact. Try Frank Sinkular again. Dave Wallick should be free now. Try to get dates agreed for a late October or early November trip.
4. Keep going on MATLAB tutorial. Code the numerical model for risk--effort pricing equation. Code acid tests. Find an equilibrium and fill in the blanks remaining in the draft paper.
5. Schedule a meeting with Dr Martin; check department requirements for confirmation of status.
6. Crosstalk article: immediately after submitting to ACSAC, write the interpretation of the first case study in terms of accreditor behaviour incentives. Write a preliminary overview of second case study based on final reports from NSA I173 and I733 (from memory; the reports themselves are classified).
7. Send out second group of US government accreditor surveys. (What went wrong the first time?) Look for UK government accreditor names in old project records.
8. Get the other two planned surveys done for background on the case studies.
9. Make a fault-tree diagram for R-prime and S-star.
10. Draw up an org chart for R, R-prime, S-star, R-double-prime, N, L and G.
11. Update anonymisation code chart (see above).

12. Finish methodology chapter (waiting on final survey questions).
13. Write first draft of confirmation report and send to Dr Martin.

To be done as soon as possible:

14. Update dissertation Table of Contents.
15. Collect examples of written work for confirmation evidence.
16. Compare NIST SP 800-53A to ISO 27001/2.
17. Update the schedule.
18. Submit forms and written work for confirmation of status during Michaelmas term.

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

End of WAR 0151.

References