File 20110211.0458: Weekly activity report 0175:

weekly activity report 175 (loughry)
Joe Loughry
Sent: 11 February 2011 04:58
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org; chip.auten@comcast.net; edloughry@aol.com; diane@dldrncs.com; Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com

Weekly activity report no. 20110210.1808 (GMT-7) sequence no. 0175, week 4 HT

The R’’ developer called an all-hands meeting this week with the new Vice President of the newly created C4ISR division now designated I2S. Under I2S, the RM programme is to be merged with TMAN under the TSS banner. (I have details of the organisation chart in my notes but do not reproduce the confidential details in this report.) The presenter at the all-hands meeting was the same manager, referenced in a previous report, who decided that the RM and TMAN programmes should be merged into a single CDS offering, and the one interesting thing about this meeting was that the new VP appears still intent that the two programmes be merged. The previous VP, over what is now the TSS organisation, is newly in charge of an internal science resource organisation that will be spreading advanced technologies into the development organisations. It is believed (by the vice presidents) that this will lead to a smooth melding of the two CDS products and no effect on current users of the systems. The R’’ developers are less sanguine, pointing to vast differences in software engineering culture, certification and accreditation level of effort, IV&V and technical approach. The chief architects of RM and TMAN have been directed to present to the new division manager a plan to merge the systems and to report monthly on progress finding synergies and commonalities that can be exploited immediately for cost savings. In my opinion, the new division manager sounds like a motivational speaker and I have never heard so many buzzwords.

On an unrelated topic, but a refreshing example of close reasoning, I read an article by Vladimir Karnozov titled (in translation) ‘Analysis of aerodynamic layout Chinese fighter J-20’. The author infers the likely mission of the new Chengdu J-20 aircraft based on the relationship between its centre of gravity---deduced from the location of the landing gear---and the canard positioning and engine air intake length, all features visible on photographs of the plane from its first public flight in January. He concludes that the J-20 was purpose-built for attacking aircraft carriers with anti-ship missiles, given its flight characteristics of Mach 1.4--1.6 supercruise, internal weapons carriage, front and side aspect (but not rear) stealth and the combination of engine performance and fuel capacity, none of which have been officially released. The performance profile this aircraft must necessarily have, given its control surface configuration and the known power of available engines fits neither a bomber nor an interceptor nor a fighter, but it does fit the profile of an aircraft designed to evade AWACS, CAP and destroyer screens around a carrier air group. The argument was brilliantly reasoned.

I met with Dr Martin this week to discuss progress, reading and plans for my trip in March. I reported that in all the reading I have been doing on grounded theory, sources are beginning to repeat themselves---I keep coming back to the same references to certain papers, books and articles. This is an indication that I am getting to the bottom of the literature. I have been playing with the software tool, ATLAS.ti, trying out different ways of coding sentences, phrases and attributed quotations.

The methodology seems to be ‘keep coding smaller and smaller units of interpretation until a new class of links suddenly becomes obvious’, which is vague but I think I am getting close to understanding the idea behind grounded theory. I am getting to the point where I can apply it.

I brought up the problem of connecting remotely to the ISPP seminars each week. The connection with OII was supposed to facilitate recording and streaming of video from the seminar series, but the equipment has not worked technically so far. Yesterday’s seminar was recorded; Dr Martin sent me a link to the audio so I could listen to the lecture. I was grateful not to miss it; Professor Sasse is one of the people suggested by Dr Flchais and Dr Jirotka who might be external examiner for my viva. The mailing list for reading group stopped working a few days ago; I forwarded information on the error to the support desk at Dr Martin’s suggestion and they were able to fix the problem. We talked about external examiners for a while; Angela Sasse is a well-known user of grounded theory in software engineering, at least since 2001--2006, and a lot of the introduction to the methodology that I have obtained is from papers by her and collaborators.

I did not have much research progress to report this week because of interactions with the Air Force sponsor who is responsible for the majority of my funding on the Probabilistic Redaction project. Last week the sponsor called to ask for a great deal of information on testing, metrics and status of development; I was provided with a PowerPoint template and spent hours helping craft a set of slides for a presentation that the sponsor had to deliver on Tuesday. By Friday the sponsor was very happy with the technical content and told us so in no uncertain terms. I was surprised then, when on Saturday night he called in an extremely upset state, saying he was unsatisfied with our progress and felt misled. I worked the weekend on a list of questions he supplied that had resulted from an internal review, and by Monday night the sponsor was once again happy with the resulting report. This was my first experience dealing directly with a funding sponsor, and it ate up a lot of time. The only research work I got done in between was reading. Late update: the Air Force sponsor contacted me later in the week to relate that his presentation to the Technical Council went very well and the metrics were accepted by the chief scientist. He is happy with us again and my funding remains stable through September. I have a meeting with the project manager tomorrow to plan work for the next three quarters.

Dr Martin warned me to beware of the point of diminishing returns when reading; there is always one more thing to read. We discussed the trip I have coming up to the UK in mid March, and what finished pieces of writing I could bring with me at that time to get some assurance that I am on the right track with the new methodology. I agreed to write up a schedule and send it to Dr Martin by tonight (see below for details).

The Oxford Security Reading Group will meet next week for a paper suggested by Anbang. Reading Group did not meet this week. I received an email from Julie Sheppard about registering for Confirmation of Status before 29th April. She sent me a copy of Prof. Kwiatkowska’s handouts from a talk to be given later in the week.

I was disappointed to miss Dr Ker’s departmental seminar this week on steganalysis, so I read the published paper that this talk seems to have been based upon. The authors found that steganographic channel capacity (to the upper limit of detectability) appears to be different in kind from Shannon’s limit on the information capacity of a noisy channel. ‘It is not the payload itself which is detected by steganalysis. It is the changes induced by embedding which are detected, and capacity is more properly given by a bound on permissible changes...' [Ker et al., 2008a]. Surprisingly, detectability increases slightly with cover image size, but is proportional only to the square root of the cover size, and is definitely sub-linear. The steganographic channel rate, they say, is best measured by the number of available embedding locations (in JPEG covers, that would be non-zero DCT coefficients remaining after lossy compression). It is thought that the fundamental steganographic channel limit is $\sqrt(N)\log(N)$ but that has not been proved yet.

Professor M. Angela Sasse of UCL gave the Information Security and Privacy Programme seminar this week, on the topic of 'Human-centred identity---rhetoric vs reality'. I was able to listen to Dr Martin's audio recording of the seminar a few days later. Besides the examples of grounded theory I have been examining in her published articles, Prof. Sasse has been working with the Cabinet Office on a replacement for the UK identity card.

The old concept of usability, she said, has shifted to one of 'user experience'; it is not enough to automate a correct and efficient process if no one will use it because either they misunderstand the benefit of it or see no reason to use the system. Her PhD student, Adrian Rahaman, interviewed policy makers, designers and developers and found that policy makers assumed that usability was something that designers and developers would automatically build in to a system. Developers, on the other hand, assumed that the specifications they were given already contained enough usability, because usability was a requirement. The disconnect led to 'undermining the policies that the policy makers started off with.' (The example given was from several London transport systems including Oyster card and congestion pricing.) Usability needs to go into the specification, said Prof. Sasse. With biometrics, policy makers are making the same mistake again. In order to accommodate the limitations of available biometric face recognition algorithms, all sorts of usability barriers are placed in the way of users, every small delay of which contributes to a longer queue. Sometimes, she said, the only user that the system is designed for is the system administrator.

Next she talked about DNA, retinal or iris imaging, and fingerprint matching. In a recent analysis of ten years of DNA matching in one U.S. state, it was found that ten percent of DNA matches were incorrect. Similarly, fingerprint matching experts have recently shown to be inexact, inconsistent and ineffective. The public have misperceptions of the reliability of DNA testing and digital signatures in court cases. The average person does not understand how DNA matching or digital signatures work, so they think the techniques are infallible.

Considering polymorphism, can the data be used in ways it was not at first intended for? In Germany, they were careful to choose the DNA markers selected for storage to make it impossible to infer the ethnicity of a person from DNA records---whereas in the UK, enough information is stored to make the same inference possible. It is even true that some people who believe in the efficacy of iridology fear that iris identification systems could leak information about health conditions believed (incorrectly) to be visible in a person's eyes. She gave more examples of unintended consequences extending from nomads in the 1920s to Facebook news updates.

Their continuing research is a work in progress. The assessment of whether a property should be rated high or low has not been developed yet, and preferably should be tied to objective criteria. They also need a mapping of profile of levels to acceptance; they have looked at a few profiles so far, but not all combinations of values. It is also becoming clear that they haven't identified all the properties yet.

Next scheduled meeting with Dr Martin is for Wednesday, 16th February at 1700 Oxford time. The chapters I would like to bring with me in March are Chapter 2, the literature survey (including all new material on grounded theory and qualitative research), Chapter 3 on methodology and most of Chapter 4 on the first case study. Chapter 4 will be incomplete, but it will contain a description of the R'' case study, the data, and the preliminary analysis. I have a month to write the new material for these three chapters. I will update the outline for Chapters 2 and 3 this weekend.

My current tasks, in priority order, are:

1. Update literature survey with references on grounded theory and Qual. research.

2. Finish more reading.

3. Import remaining R'' case study source material into ATLAS.ti.

4. Figure out a way to make event traces in the H. unit linkable.

5. [Waiting] Figure out if I can use the chronological record in my lab notebook as a source for the 'memo writing' activity that occurs later [not done yet]

6. Plot tasks on a new Google Calendar as blocks in a 168-hour week. Establish limits on non-thesis work times. [I need this now. It was delayed by Lockheed work. It will be done by Monday.]

7. Outline the survey journal article that the assessors asked for. I still need to find some good examples of how to write a survey article [not started yet]

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

End of WAR 0175.

References