File 20110304.0449: Weekly activity report 0178:

weekly activity report 178 (loughry)
Joe Loughry
Sent: 04 March 2011 04:49
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. 20110303.1615 (GMT-7) sequence no. 0178, week 7 HT

GSS report for Hilary term has been submitted. I kept the report short this time, as all the detail is in the weekly reports.

I received a letter in the post from the University regarding confirmation of status. It seemed to state that I must apply before the end of Hilary term, which is 12th March. I am being forced by the calendar and I dislike that. All week I have had a very bad flu or a cold, but I am working in spite of it. I asked Dr Martin about the letter from MPLS and whether it meant I must submit a report before it is ready.

Dr Martin and I met Monday at 3:00 PM. I had prepared an agenda organised around re-planning all work to get the confirmation report submitted next week. That turned out to be a false alarm, as the report is due Easter, not next week. For future reference, ‘the end of week 8’ really means ‘before week 0 of the following term’. I will have chapters and the confirmation report ready by that time. We talked about what ought to go into Chapters 1 and 2; Dr Martin said some people put a lot of material into the first chapter about why their problem is interesting; I need to fix up my outline of Ch. 1 and balance it over Chapters 1--2 more evenly.

I was advised not to prioritise the GSS report over productive work. The details should come from my weekly reports anyway. He sent me a link to the MP3 of last week’s seminar on cyber warfare, a good thing to do when I am sick in bed. I am going to try to get over this flu and get back to productive work.

The set of issues identified in support of the grounded theory of the R’’ case study keeps growing. The programme manager, and hence by extension the government programme office (GPO), sees the following issues: budget, cost of certification [forced more by vendor OS product cycles, which are themselves forced by vendor hardware product life cycle, pincered from the other end by government insistence on OS certification, which is slow and affected by both CCTLs and the requirements of the CCRA and NIAP CCEVS], many site installations on hold waiting for a certified CDS before they can get ATO, a developer who sometimes does not work as quickly as the GPO would like, and developer engineering overhead costs.

The developer, on the other hand, sees a different set of issues: the same vendor OS product cycle problem as described above, but also software engineer hourly cost, overhead ‘tax’, award fees and the Contractor Performance Assessment Report (CPAR) rating, the problem of keeping engineers current, travel budget [always a difficulty], lots of installations all over the world, IV&V and government regression tester performance, opaque penetration tester minds, and the unique mode of operation of pen testers, which are like terminators: they absolutely will not stop---ever---until they run out of money.

There is relevant material for my dissertation in the article on the GBU-28 crash development programme in Kopp (2005; revised 2011a).

Contemporaneously, regarding the RM/TMAN umbrella merger, the developer's Systems Engineering manager (KM) told the developer's technical staff this week that what was described recently at the (MW) all-hands meeting a few weeks ago was not correct. [(MW)] said things at that meeting that were 'the opposite of reality.' It is not the RM programme manager's (OKJ) or TMAN programme manager's (SB) intent that the two CDSs are to be merged into a single (Next Gen) product; they will remain separate software development organisations developing different but complementary products that serve primarily, but not entirely, non-overlapping sets of customers. Previously to those remarks of the new VP, things had been going well in the sense of getting the two software development organisations to work together; people were beginning to talk to their counterparts on the other side, asking questions and sharing information, but then this speech of his caused friction within the ranks. The Systems Engineering manager reiterated to his staff that the umbrella organisation, TSS, will result in few visible changes within the RM closed area.

For example, he said, one specific instance of friction that occurred was the sharp shift in perception around the push to sell the MAG component of RM as a service or library to TMAN. Lots of people got on board with that, RM developers were talking with TMAN developers and information was flowing. When the story changed slightly to say that TMAN would incorporate the MAG library for free, sharing ceased. The rumour was not true; in point of fact MAG will be sold to TMAN just like any other outside entity, and the revenue will be booked to RM under the TSS umbrella. It is not about merging the programmes. In a later conversation, the Systems Engineering manager had some interesting remarks to say about Lockheed Martin (LM) and its competitors in the CDS market. LM, he said, does not understand guards at all, as a corporation. The RM organisation understands them because it makes an extremely flexible guard that has been installed in countless different environments; the TMAN organisation understands them a little, because it makes a special-purpose device that is installed in only one specific kind of environment for the benefit of a single and homogeneous customer. Raytheon, the strongest competitor of LM in the CDS arena, gets it. At conferences, the Raytheon booth on display sprawls across an area half the extent of the RM developer's entire closed area, staffed with dozens of uniformed (business casual) Raytheon employees who will talk to anyone about their product, the Raytheon High-Speed Guard---with the exception of the RM developer; Raytheon will never talk with the RM developer at conferences, despite the RM developer offering to share information. In contrast, Lockheed Martin's booth at conferences is the size of a large closet, and that space is shared between RM and TMAN. He listed the main competitors in the CDS space, in order of share, as LM, Raytheon, Boeing [Hardwall, a product they bought from somewhere], and ISSE. (ISSE seems to be going away.) RM is unique amongst the competitors, being the only single-box solution; all of the others require multiple boxes (multiple boxes cost extra space, weight, air and power); Boeing Hardwall in particular deploys a box for every flow, even in a simple bidirectional flow situation. [It's a design trade-off; I can see accreditation reasons for doing it that way, in the view of some DAAs.] An interesting story came out of the discussion that I had not heard all the details of before: a few years ago, Raytheon lost a lawsuit brought by Lockheed over the Raytheon High Speed Guard; according to the story, some Raytheon engineers had called the RM technical support telephone number asking for help with the RM software, but according to Lockheed Martin's records, they did not have such a unit. By unfortunate happenstance, the person who answered the phone that day was the RM programme manager (TF) and the industrial theft was discovered. Raytheon, according to the story, later reverse engineered the RM CDS and subsequently claimed compatibility with MAG in their advertisements. (I have a copy of that advertisement.) The settlement of the lawsuit, it was related, specifies that should Raytheon ever offer a CDS, it must be built of components 80 percent code-different from RM. (I would like to get more formal definition of those terms.) To get the whole story, I plan to go to the sources (JP/F and TF); I have one meeting arranged so far to get the details. I am not completely sure it is relevant, but one of the tenets of GT is to feed in everything.

The post-certification patch, version 5.01, is done; testing and CR verification is going on now, but reports so far are that the build is solid. FAT dry runs will occur before RMUG, an event which takes place the first week of April; FAT will commence immediately following RMUG. The patch fixes a slew of the kind of small bugs that seem only to be discoverable in production; there have been no major problems discovered in production since the first post-certification accreditations were done on 5.0 immediately after UCDMO base-lining and TSABI approval.

The Oxford Security Reading Group met this week primarily to discuss preparations for the department's Open Day, but also for the Infosecurity Europe show in April. Before things got going this time, I told the rest of the group about a new paper I read by Wei, et al. (San Jose, California: FAST'11, 15--17 February 2011) on securely erasing SSD and other flash storage. The researchers studied the interaction between wear levelling and secure erase in these devices by reading the chips with a custom FPGA hardware interface to bypass the Flash Translation Layer (FTL) under the CHS interface. They found up to sixteen copies of identical stored data in non-user-accessible regions of storage and showed that the ATA security commands ERASE UNIT and BLOCK ERASE do not always work, as a result of bugs in the drive firmware. There was a discussion of this paper in Schneier's blog the other day; one of the comments contains a detailed description of the engineering of a thermite destruction mechanism for secure storage, interesting for the thermodynamic and safety considerations that obviously informed its design.

11th March is the deadline for signing up for a slot in the Open Day programme. Shamal suggested a poster 'Towards an Information Security Institute' and we discussed likely visual images for each of the research topics (example: 'observing a point of connection' for CDS), including Webinos. The message of the Infosecurity Europe exhibit, said Dr Martin, is definitely about course offerings, but some space could be set aside for research opportunities at Oxford. At the Open Day, we will have much more space for research. Might there be anything else coming up, asked someone, where we could display a poster designed for this purpose, and make it serve double duty? I asked the group what message we are trying to put forth; who are the people likely to attend Open Day, and do they differ as a population from attendees of the Infosecurity Europe show? Answer: Open Day attracts large businesses and small local businesses, plus a few people from Cambridge. From my perspective of working for a very large company, Lockheed Martin has a continuous need for variable-term, extremely short lead-time expert help on an astounding variety of topics, and [if they knew about it] the company would benefit from knowing what projects are active in the University. Company managers would want to have two things: first, a pre-existing contact arrangement, since often the need is urgent, especially on proposal work; and second, a willingness to enter into short-term subcontracts of only a few days or weeks duration. This is different from the usual industry--University relations, which are more oriented towards sponsorship of larger research projects or facilities. The comlab is full of people who could validly sit in for a few hours of a 'red team' review on an important proposal, giving an adversarial viewpoint on the suggested design before it goes to the evaluator for selection. All the necessary background is provided by these proposal efforts, a necessary consequence of the fact that they always want outsider perspectives; as a plus, the proposal manager usually has more money at his disposal than time. I will put a version of this on the wiki that John set up.

Dr Martin said we should reserve a slot for the Open Day. The Infosecurity Europe show is more urgent, the week before Easter; it is 2--3 days turnaround time on poster reproduction. Video call ended at 0543 AM.

I listened to the audio recording of last week's ISPP seminar given by Prof. Peter Sommer from LSE on 'Defining CyberWarfare'. 'The subject has changed remarkably little' [since 1996], he told us. Back then it included new battlefield technologies, concept of a new doctrine, industrial espionage or competitor intelligence---the 'irregular verbs' of Bernard Woolley---psychological warfare, logical and physical attacks on systems. Prof. Sommer acted as the defence expert in the 1996 trial of two UK teenagers under the Computer Misuse Act for a 1994 incursion into USAF systems that had been routed through Columbia, Latvia and South Korea at least. The attack was mistaken at the time for the actions of a large state actor. Names are important, he said: cyber warfare (a strictly military problem) vs cyber crime (oh, it's a law enforcement problem) vs cyber security (it's just a problem for the techies to solve) vs cyber incidents (can be almost anything). Gilbert Ryle's 'philosophy as cartography' (from The Concept of Mind) regarding different definitions of the word 'possession', is a good example.

The presenter gave a brief overview of UK and European laws applicable to computer-related, -mediated or -facilitated crimes. The treaty of Budapest (or computer crime convention) in Europe; in the UK, 'the Computer Misuse Act is there when no other regulation is available'; the principle is to prosecute for the substantial offence rather than the modus operandi. (This is not dissimilar of the definition of risk responsibility given by Ross Anderson in his book on security engineering, I thought.) The Fraud Act of 2006 is used for money laundering, phishing, identity theft, and DDoS extortion. Many taxonomies of cyber attackers have been published; the absurdity is clear if you look at the analogy to 'car crime'. The presenter gave lists of surveys and articles attempting to build up the problem; cyber incidents...nobody agrees what sort of incidents to count as part of an attack, how to figure the cost of clean-up, compensation of third parties, loss of revenue, or the really nebulous 'loss of business opportunity'. There are lots of definitions, but no coherence.

The situation is similar regarding cyber warfare. These researchers limited their definition to something more akin to 'kinetic' attack: UN charter Article 51 provides for certain circumstances in which people can retaliate: it must be militarily necessary, it must be proportionate, and it must avoid collateral damage to innocent third parties.
The problem of attribution is the biggest one: [it occurs to me that] cyber warfare attackers do not wear uniforms interpretable by the enemy.
I liked this statement of Prof. Sommers': 'If you can't figure out who is attacking you, that means that you have to think about a completely different form of defence...resilience and contingency planning.'
To this researcher's group, the term that particularly appealed was 'cyber weapons'. Discussion of capabilities, qualities and limitations of cyber weapons. A nasty substance is not a weapon until it has been weaponised, which means it can be controlled and directed.

Taxonomy of motivations for deployment: recreation, propaganda, [civil disobedience is a new one here], demonstration of illegal power and intent, disruption of activities [e.g., Stuxnet], as a force multiplier for kinetic attack, espionage, or criminal purposes. Reasons why people go to war. Stages of war, from recalling of ambassadors to UN resolutions to the staging of exercises off somebody's coast [this is the point where cyber weapons probably start to be quietly employed, said Prof. Sommers], insurgency, brief attack followed by a pause, and then total war. In the near future, there could be a cyber element to offensive operations as localised as a political assassination. That is an interesting thought.

In the question and answer period afterwards, there was a question about attacks by state actors against private companies. In the context of answering, the presenter said that he feels 'there is a good argument for countries to have a cyber weapons offensive capability and the reason would be if it is very well researched, if it is very well targeted, it has the benefit that it might be able to stop something worse without too many people dying.' Later, he noted that the private sector is far advanced over the public sector in the area of resilience and contingency planning, the only defences that work against an unattributable attacker.

My next meeting with Dr Martin is scheduled for Tuesday, 8th March at 3 PM Oxford time.

My current tasks, in priority order, are:

0. Get rid of this cold.

1. Detailed outline of Ch. 2, 3, 4.

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

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 [on hold].

5. How can I can use the chronological record in my lab notebook as a source for the 'memo writing' activity that occurs later?

6. Plot tasks on a new Google Calendar as blocks in a 168-hour week. Establish limits on non-thesis work times [finally getting to this].

7. Survey article needed for summer [not started yet].

8. Planning for confirmation report that is needed sooner than I thought.

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

End of WAR 0178.

References