File 20091008.2206: Copy of weekly activity report 105:

Weekly activity report no. 20091008.2000 (GMT − 7) sequence no. 0105, noughth week MT

I met with Dr Martin yesterday after Reading Group. We discussed progress on the Air Force request-for-information (RFI), the response to which is due 16th October. Right after our supervisor meeting, I met with a former Project Manager (PM) of the project described in my first case study at a coffee shop; he and I talked about the RFI (more so than about the case study which was my original purpose in getting together). As soon as I got back from that meeting, I had a telephone message from the PM who is coordinating the RFI response. She said Lockheed management have become interested and asked for a summary. I have not written anything down yet, but while I was talking with her on the phone, it crystallised and I knew what to say. The RFI asks for a solution to the DIACAP problem (the US DoD's latest certification and accreditation (C&A) standard). Nothing like that currently exists, which is part of the reason why C&A is so unaccountably expensive. The UK Ministry of Defence, via CESG and reporting through Whitehall, almost certainly have such a system already. The British way of doing C&A has historically been different from how the US does it—more risk-driven than testing-based; therefore, I conclude, MoD must have a process like the RFI is asking for already in-house. It might not be automated to a very great extent, though. I don't have any knowledge of that UK system. Its existence is merely a logical deduction. (Deduction or inference? I need to sort out my terminology.)

Potential competitors: IBM will undoubtedly pitch a Lotus Notes-type workflow solution to the RFI. That's their consulting bread and butter. Microsoft will say they can do it all with SharePoint. Both of those efforts will tie up buildings full of software developers and systems engineers for years working on it. But it's not what the RFI is really asking for.

DoD needs something now. The RFI asks for an Air Force tool to handle accreditations under their AFI33-210 process (a tailored DIACAP). It simply can't be only the Air Mobility Command that needs it. Reading between the lines, Air Mobility Command got stuck with the RFI because nobody else wanted to do it. They brainstormed up 86 requirements with no functional framework, but obviously representing the specific, immediate needs of a small group of C&A practitioners who are buried up to their eyebrows in past-due work.

This is not just the US Air Force. DIACAP is DoD-wide; every combatant command has got the same problem. Unlike the intelligence community, DoD pushes responsibility for C&A risk acceptance down to the individual combatant commands. Solve this, and every combatant command will want one.

I figure conservatively 4 to 7 times (a purposely low number) of that many accreditations across DoD—based on the relative size of the services and their current activity—as were called out in the RFI. Fortunately, I think I can architect it to handle 10 000 simultaneous accreditations as easily as 200. (That is historical as well as current accreditations.)

I have been thinking about this exact problem—although from a Common Criteria perspective instead of DIACAP—since 2007. I have a year to demonstrate a working prototype before I have to write my dissertation and defend it. Coincidentally, that matches exactly with Fiscal Year 2010, so there is a possibility of funding to develop it. An excellent response to the RFI is a necessary but not sufficient condition for that funding. I will describe a software system achievable in the next year by my own effort that nevertheless is fast, reliable, and future-proof. We can stream in an update in a couple of years, firmly based on observed and measured usage metrics, without disrupting the users who by then will be depending on the continued smooth operation of the system.

Plan for this week: I must concentrate on writing the RFI response. Today, I finished a quarterly status report that I owed to another project, but now that that's done I can focus on the RFI response. A slightly modified version will also be submitted to Crosstalk as an article.

Finally, I described what I've been reading over the past week. I am trying out a method called 'Getting Things Done' for organising tasks. I have the book and an empty stack of file folders; I will report the level of efficacy later.

Next meeting: Monday, 19th October at 7:00 a.m. Oxford time.

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

References