File 20111202.0720: Weekly activity report 0217:

weekly activity report 217 (loughry)
Joe Loughry
Sent: 02 December 2011 07:20
To: Joe Loughry

Weekly activity report no. 20111201.2226 (GMT-7) sequence no. 0217, week 8 MT

Dr Martin and I met via Skype on Wednesday; I reported that the AFRL sponsor notified me yesterday that 'Probabilistic Redaction' will be published as a journal article next year; it is undergoing peer review now. I reported some progress on thesis work in the area of formal and informal systems (interview with a new informant) and we discussed it in the context of email retention policies. I reported that I have been working on the certification process model but having trouble making what Dr Flchais wants, and that I had arranged to call my co-supervisor the following day. Tuesday, I met with managers at Lockheed regarding transition plans. I will fax the GSO.15 form for time extension, as expected, to Dr Martin tonight. Next meeting scheduled for 7th December 2011 at about 5pm Oxford time.

The security reading group met this week to discuss the Applidium report titled 'Cracking Siri'. I was interested in this report because the Siri functionality sounded familiar when it appeared a few weeks ago; sure enough, Siri is actually PAL---a DARPA project from 2003 with a number of papers written about it. Andrew Paverd mentioned a paper he'd read on speech-to-speech natural language translation that focussed on shifting electrical power requirements from client to server; like Siri, PAL unloads processing from the client to save battery capacity in the field, an important design consideration for tactical devices. Originating as it did from a DARPA request, the power consumption trade-off seen here suddenly makes sense. The protocol observed over-the-air is an interesting combination of security and openness; Cornelius speculated that the ease of hacking it may reflect a design decision of Apple to open it up a bit more later, as the client accepts a certificate signed by any root CA. The ACE HTTP method used here suggests to me that SSL proxies used by organisations to look inside HTTPS connections through their firewalls are more lenient than I would have thought; Apple must have tested this connection method extensively and chosen it for maximum interoperability, but what it tells me is that MITM firewalls are monitoring, not enforcing. Andrew Paverd wondered what other sensor data the iPhone 4S might be transmitting along with the device ID, text, and raw voice. The apparent openness of the protocol may reflect an intention to extend Siri service eventually to devices that lack unique IDs; tablets look like phones to the network, but laptops don't. The interesting part of this report was not the hack itself, but all the questions it raises.

I met with Dr Flchais for an hour Thursday via Skype. I first briefly updated him on my work finishing the probabilistic redaction project for the Air Force and the effect it had on my thesis progress. Then we got down to work. We had a long discussion about grounded theory. The place where I am stuck is at the stage of modelling and validation of models. I have got about as far as a person could be expected to get in isolation, he said; it is time to begin collaboration in earnest, and regularly. It is the only way to achieve good models. Dr Flchais gave me three ways to validate, and I related how I have already done some of the third type. Documentation of it is key for the examiners, though. It was agreed that I should immediately begin coding CS-1 in ATLAS.ti. The size of my data is unusually large, which causes a problem for

grounded theory; Dr Flchais wants to see regular reports of percent completion of the raw data items beginning immediately. I promised to provide them; by tomorrow I will have a rough count of CS-1 and begin to report status in the requested manner. Dr Flchais will be closely involved in the categorisation step.

We talked about specific methods for interpreting data. I recorded much more in my notes after the call. From here on out, it will take very diligent focus to complete on time, but I was assured that the drastic measures I have taken recently are the right ones, and the result will be a high quality dissertation. It was an extremely helpful meeting.

Joe Loughry
Doctoral Student in the Department of Computer Science
St Cross College, Oxford

End of WAR 0217.

References