File 20111011.0630: Notes from security reading group, 0540 this morning, on the paper 'Automating Security Mediation Placement' by King, *et al.* (2010), suggested by Cornelius.

Interesting discussion part-way through the discussion on implicit *vs* explicit information flows. John and Justin really got into it; Justin in particular was in good form talking about TaintAndroid and the difficulty posed by side channels. I challenged his assertion that if we eliminate all the explicit information flows, then the implicit information flows will immediately become visible, because some sort of measurement of aggregate information flow would be needed, and that would probably require an instrumented processor. If attackers can find implicit information flows, I said, why can't we? Justin and I both came to the same realisation at the same moment and shouted it out: the imbalance comes directly from the fundamental asymmetry of the attacker/defender perspectives (the attacker need only find one weakness to get past the defences; the defender must anticipate all possible attacks and defend against them all).

John brought up aspect-oriented programming and we all had a good discussion of that.

No paper proposed yet for next week; Justin was talking about the MULTICS paper and might suggest that as an historical paper.

References