File 20090407.0901: Notes from the *Trust 2009* conference, St Hugh's College, Oxford:

Prof Sean Smith: a lot of what is taught in software engineering courses is rubbish. 'Use what works and throw the rest away.'

Crypto *device* validation: never trust a vendor. Finite state machine: a glorified flowchart.

They used ACL2, but Prof Smith wishes he had used a model checker and used it earlier.

Rant: standards are too detailed and at the same time not detailed enough.

Quote: Carl Ellison (?) said, 'You're going through all this protocol to prove you're running Windows. Why not just admit it?'

Rant: SE Linux security policies are still at the usability level of assembly language.

Abandoned(?) experiment: timing attack against a TPM: it took 40 days to do one experiment.

Next talk: Marcel Winandy on Common Criteria validation of a Protection Profile (by the German *Bundesamdt...*) at EAL5.

HASKPP design goals:

1. PP as minimal as possible to allow for differing implementations.

2. Prevent 'trivial' realisations from claiming conformance.

Balancing these two design goals was a challenge throughout.

References