File 20090408.0943: Notes for meeting with Dr Martin tomorrow:

- I would like to send Green Hills Software a book proposal.
- I don't need a contract to research a book, only access.
- I have been talking with Prof Cynthia Irvine, one of the authors of the SKPP.

Mike Just gave a talk about challenge questions at Trust 2009. I admire their methodology: they designed the experimental protocol so that the experimenters did not gain access to the subjects' challenge question answers (only the questions). This is admirable in view of the cavalier attitude towards personally identifiable information (PII) today.

How would you calculate the entropy for *my* preferred sort of challenge question? (Mike Just: 'they must hate you'. I like to make my questions things like, 'Roman numeral VII, potassium ion, and a small blue toy giraffe on wheels.' I try to come up with a string that's not even representable in Unicode. Although, if the description I just gave can be encoded using no more than 26 distinct (case-insensitive) English characters, that doesn't get around Shannon's estimate of 2.3 bits of entropy per character. It's just a passphrase, albeit an unlikely one to fall to a dictionary attack.

- Talk to Ahmad-Reza Sadeghi about the HASK-PP Common Criteria evaluation. He was the first author on that paper.

References