Session 4 (and other stuff)

- Session 4 raised some issues that are relevant more widely than just in ID
  - Diego: diversity is a good thing; things *will* go wrong; statistical evidence is important way of showing that things work…
  - Roy: testing; evidence; evaluation; decision-making; dependability case; *numerical* claims; costs…
- So…some associated wider issues:

Issues in security assurance

- Some contrasting views:
  - ‘Completely’ *vs* ‘adequately’ secure
  - Proof/reasoning *vs* measurement/assessment
  - Process *vs* product
  - Achievement *vs* assessment
  - ‘More secure’ *vs* ‘how secure’

Issues 2

- ‘How secure’ implies inevitability of uncertainty (is this true?)
  - How do we handle uncertainty?
- Is *probability* the right formalism?
  - If not what?
    - Fuzzy? Dempster-Shafer? OMDB…!

Issues 3

- How do we express claims?
  - For *reliability,* for example, we have: R(t)=P(no failure in time t)
  - What replaces ‘t’ for security?
    - *Not* time: effort? This is a difficult problem (I’ve worked - fairly unsuccessfully - on it)
    - If we agree *what* it is, can we measure it?

Issues 4

- How do we use evidence to support claim?
  - Evidence very disparate - statistical, logical, judgmental, qualitative and quantitative…
  - How to combine all this into an argument to support the claim?
  - ‘Security cases’? Bayesian Belief Nets?

Issues 5

- Diversity is A GOOD THING
  - But *how* good?
  - Diversity does *not* give independence
  - Thus need to know level of dependence
  - Trade-off between dependence and version ‘reliabilities’
  - Can any of this be measured?
  - Are models from reliability and safety relevant here?