File 20111108.1020: Notes from Dr Calloni's LM-VTIS today:

I talked with Dr Ben Calloni about a talk he gave at IEEE METROCON 2011 on 'Automated Vulnerability Path Assessment'. Their research has not been published yet but contains a method for systematically deciding whether to accept the residual risk in an accreditation, using a mathematical approach to address the weakness space.

He said in response to a question about the Common Criteria that the reason companies go to international schemes for evaluation is because the NSA evaluators and validators that oversee NIAP CCEVS have it as a secondary duty; this causes events to be postponed when other work becomes more pressing. Vendors going overseas for their evaluations do not have that problem.

> 'A vulnerability without a threat is not a risk.'

—Ben Calloni.

References