File 20101214.1030 (MST): A collection of interlocking models and metaphors. There are several levels of metaphor here, and the problem can be viewed in light of any of them. At the apparent observant level, we have a lot of government, military and software development people arguing over a problem of penetration testing and risk analysis. At a slightly more abstract level, we have a risk market, existing necessarily as a result of the presence of asymmetric knowledge, one of the things proved by Stigler in 1961 and applied successfully by Akerlov in 1970 and Spence in 1973. But markets are tricky things, and I needed something a bit more measurable, so now we have another metaphor, a physical analogue, that when perturbed in a particular way exhibits behaviour strikingly similar to observation in the case studies. So we come full circle, with a validation of the theory that is at the very least suggestive.

The model of accreditors with different security clearances is not a metaphor, but it is a useful model.

So that is where I am. I searched a long time for a model that explained these observations.

Serious, sober, matter-of-fact, confident, assured; expert with facts, events, theories, references, names and dates at your fingertips.

This dissertation is a moving target. The report you received earlier is a fair representation of what I was thinking at the time, but I would like to use that report as a jumping-off point to tell you what I am thinking now.

A cross domain system is a controlled way to violate security policy. It is the dual of a covert channel, and obeys many of the same rules. It is what they needed to prevent information from leaking out like it did to Wikileaks.

References