File 20120110.0635: Notes from reading group:

Reading Group met this week to discuss 'Looking Back at the Bell–LaPadula Model' by David E. Bell, from 2005. The paper explains the reasons for several apparently mystifying decisions in the TCSEC and shows how they came about, like the 'compatibility' of ordered security levels in a filesystem hierarchy; it was named that because the decision was made by programme managemement fiat against the recommendation of Bell and LaPadula, who wanted it to go the other direction. It always baffled me why Trusted Solaris 2.5.1 was that way; now I know why. I gave the group a rapid overview of multi-level file systems and the software developer's opinion of privileged processes. The mystery of why Information Labels (IL) disappeared between Trusted Solaris 2.5.1 and TSOL 8 was finally cleared up. The paper contains still trenchant observations on the practical difficulty of certification and accreditation and the opportunity to place high-assurance gateways in the narrow lines between almost-isolated networks. I wondered aloud whether the 'almost-isolated networks' today were large things like Facebook and Twitter; a good question from Andrew Paverd prompted a discussion whether the entire intelligence community should be considered one, and Justin got me thinking about how one decade's optimisation is the next's bottleneck.

Duration of call: 48 minutes.

References