

File 20080703.0804: Notes from meeting with Dr Martin:

- Punch line of the transfer report
- EAL5 impossible for existing products
- existing products are not secure
- Future of Trust in Computing meeting last week
- contribution, methodology, motivation: student conference
- more case studies
- Australian guy—fully verified separation kernel
- considerably above EAL7
- i86 platform
- L4 kernel
- SE L4
- Gernot Heiser
- \$ 3K/LOC for EAL5 or 6
- Australian guy is claiming 300 KLOC
 - How does the cost break down in terms of process docs
- Exciting stuff—it's so terribly broken, and in such interesting ways, that I really want to tell people about it.

References