File 20080312.1245: Notes from Reading Group: Ross Anderson paper [1]. Applicability of the Red-Blue model to the adversarial relationship between a vendor and the CCTL?

> [S]oftware companies should hire more software testers and fewer but more competent programmers.

In section 3.1 of [1], *c.f.* CC eval and Open Source.
30 percent of large software development projects fail (citation on page 6 of [1]).

> [S]ecurity tends to be a lemons market anyway.

Landwehr paper [3]: history of U. S. Government evaluation processes: TCSEC, ITSEC, Common Criteria. Evaluations conducted at government expense by NSA, leading to vendors listing their product as 'in evaluation' but never completing the process. See also Anderson2001 [2].

> The Common Criteria suffer from different problems, most notably adverse selection: vendors shop around for the evaluator who will give them the easiest ride, and the national agencies who certify the evauation labs are very reluectant to revoke a license, even following scandal, because of fears that confidence in the scheme will be undermined [2].

Recent result: European Union Network Security Policy (see Anderson paper [1] for cite).

> The dependability literature teaches that large software project failures are mostly due to overambitious, vague or changing specifications, coupled with poor communications and an inability to acknowledge the signs of failure early enough to take corrective action [1]

> But (as with the Common Criteria) certification markets can easily be ruined by a race to the bottom; dubious companies are more likely to buy certificates than reputable ones, and even ordinary companies may shop around for the easiest deal.

References

[1] Ross Anderson and Tyler Moore. Information security economics—and beyond. In *Information Security Summit 2008*, Prague, Czech Republic, April 2008.

[2] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Computer Publishing, 2001.

[3] Carl E. Landwehr. Improving information flow in the information security market. In *Economics of Information Security*, pages 155–163. Springer US, 2004.