Homework #5

Due: June 6, 2013 (*Please, no late assignments!*) **Points:** 100

Questions

1. (*30 points*) Consider the rule of transitive confinement. Suppose a process needs to execute a subprocess in such a way that the child can access exactly two files, one only for reading and one only for writing.

   (a) Could capabilities be used to implement this? If so, how? If not, why not?

   (b) Could access control lists be used to implement this? If so, how? If not, why not?

   (*text*, problem 17.3, modified)

2. (*30 points*) A company develops a new security product using the agile programming[1] software development methodology. Programmers code, then test, then add more code, then test, and continue this iteration. Every day, they test the code base as a whole. The programmers work in pairs when writing code to ensure that at least two people review the code. The company does not adduce any additional evidence of assurance. How would you explain to the management of this company why their software is in fact not "high assurance" software? (*text*, problem 18.7, modified)

3. (*40 points*) A noted authority on penetration testing advised the testers to look on the target system for the reference validation mechanism, if there was one, or the software and hardware that implemented (approximated) a reference monitor. Why did he suggest this?

Extra Credit

1. (*25 points*) What are the conceptual differences between a reference validation mechanism, a trusted computing base, and the TOE Security Functions? (*text*, problem 21.4)

[1] In the book, this is called "extreme programming"