Homework 4

Due: March 14, 2016 **Points:** 100

1. (*40 points*) Extend the semantics of the information flow security mechanism in Section 17.3.1 (in the chapter uploaded to Resources>Textbook, 2nd Edition, Chapters on SmartSite, or Section 16.3.1 in the bound book) for records (structures).

2. (*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?

   (b) Could access control lists implement this? If so, how?

3. (*30 points*) In the Janus system, when the framework disallows a system call, the error code **EINTR** (interrupted system call) is returned.

   (a) When some programs have read or write system calls terminated with this error, they retry the calls. What problems might this create?

   (b) Why did the developers of Janus not devise a new error code (say, **EJAN**) to indicate an unauthorized system call?

Extra Credit

4. (*20 points*) A company wishes to market a secure version of the Swiss Cheese Operating System (SCOS), known as much for its advanced user and database management features as for its security vulnerabilities. The company plans to build a virtual machine to run SCOS and run that virtual machine on a second system, the Somewhat Secure Operating System (SSOS). The marketing literature claims that the VM running SCOS provides total isolation, thereby eliminating any potential security problems.

   (a) Does this arrangement provide total isolation? If your answer is "no," discuss what features the VM would need to include to provide total isolation or show why this arrangement cannot provide total isolation.

   (b) The literature states that "the VM mediates all accesses to real system resources, providing an impenetrable barrier to any attacker trying to break out of the SCOS and attack other copies of SCOS running on the SSOS." Do you agree or disagree with this statement? Why? (If you would need more information in order to make a decision, state what information you would need and why.)