

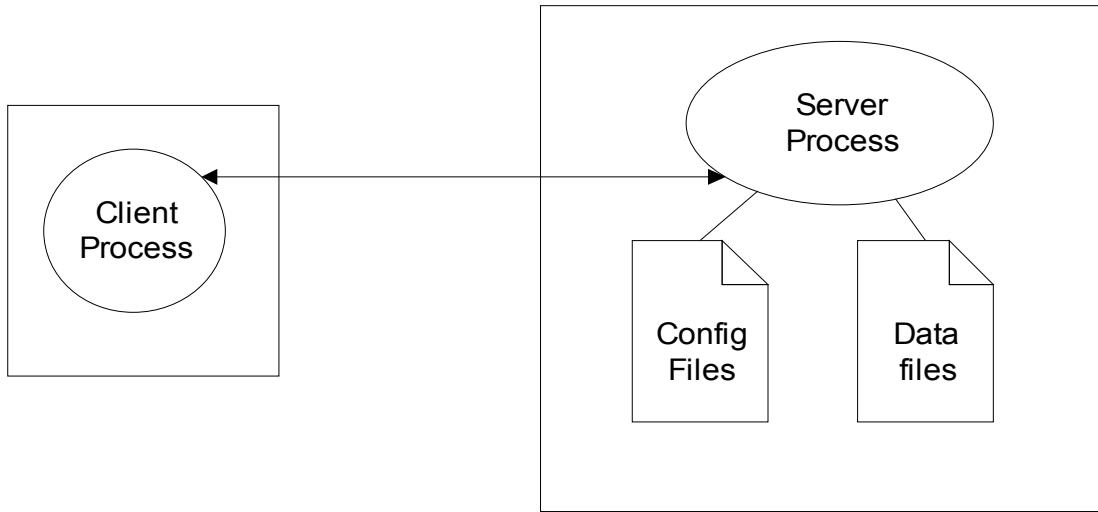
Name:

Information Assurance: Homework 6

Due October 24, 2007. Late homeworks only accepted though October 26, so we may post the answer key in time to help students study for exam 2.

1. The Type Enforcement mechanism provided by SE Linux is very general. Can it encode the BLP rules of a specific security level lattice? Consider a set of security levels with clearances $H > M > L$ and categories P1 and P2. Identify the necessary types and domains and allow statements (as defined in page 26 of the class slides) to define a Type Enforcement system that would enforce the BLP simple security condition and *-property. Or identify the weaknesses in the Type Enforcement scheme that would prevent such a mapping.
2. Compare and contrast the Pitbull LX access control mechanism and the SE Linux Multiple Category Security (MCS) mechanism. Identify one way in which they are similar, and one way in which they differ.
3. Try LibSafe to detect a sprintf() buffer overflow error. You can access libsafe from <http://www.research.avayalabs.com/gcm/usa/en-us/initiatives/all/nsr.htm&Filter=ProjectTitle:Libsafe&Wrapper=LabsProjectDetails&View=LabsProjectDetails>. If you do not have administrative access on the target machine, do not run “make install”. Instead set the LD_PRELOAD environment variable to the location of the libsafe library, /home/shinrich/libsafe-2.0-16/src/libsafe.so.2.0.16, in my case. The man page for libsafe is posted at <http://www.cs.uiuc.edu/class/fa07/cs461/libsafe.8.html>. Show problem code snippet and report on results.
4. You have been assigned the task of augmenting a virus scanner to detect the latest encrypted virus. You have an example of the virus in your isolation lab. Describe two techniques for identifying a general instance of the virus and describe one possible downside for each approach.
5. Use the threat modeling technique discussed in class to analyze a rather high level system design of a banking client server application. A system diagram is shown below. The client process can run on a separate machine from the server. The operation of the server is controlled by configuration files stored on the server machine, and the persistent data is stored in data files on the same machine as the server machine. This is very early in the design so there is no real code for you to analyze. Identify assumptions that you are making about the system in your analysis.
 - a. Identify two classes of system entry points.
 - b. Create one threat profile for a possible threat to the system.
 - c. Create a threat tree to illustrate that threat.

Name:



Banking system high level design