CSE591: Security Policy Frameworks

Scott Stoller and Annie Liu

Homework 1. Version: 10Feb2005a. Due 17 Feb 2005.

Problem 1

Consider the following scenario.

1. A user u is assigned to a role r that has permission p.
2. User u creates a session s and activates role r in it.
3. A security administrator calls *DeassignUser*(u, r).

Can u still perform an operation authorized by permission p in session s? Justify your answer, with precise references to appropriate parts of [1].

Problem 2

Consider a proposal to simplify ARBAC97 [2] by eliminating UP roles. Thus, every role must be an ability or a group. Is this a good idea? Justify your answer. You don't necessarily need to reach a definitive yes/no answer. You do need to discuss the issues raised by this proposal.

Problem 3

The article on ARBAC [2] says "The main reason for distinguishing among the three kinds of roles is that different administrative models apply to establish relationships among them" (page 122). What are the differences in administrative models for the three kinds of roles (activities, groups, and UP roles) in ARBAC97? What should the differences be (in your opinion)? Is the distinction between these three kinds of roles in ARBAC worthwhile? Justify your answer.

References

[1] David F. Ferraiolo, Ravi sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3):224–274, 2001.

[2] Ravi Sandhu, Venkata Bhamidipati, and Qamar Munawer. The arbac97 model for role-based administration of roles. *ACM Transactions on Information and Systems Security (TISSEC)*, 2, February 1999.