CS590U: Access Control: Theory and Practice Spring 2005

Assignment #5 Due: Tuesday, March 15, 2005. Email to the TA: luy@purdue.edu

Problem 1 (10 pts) People often claim that RBAC is natural to support policies such as separation of duty and least privilege. Give your thoughts on such claims. In particular, how can one justify such claims? How can one criticize such claims?

Problem 2 (10 pts) Eight design principles that can guide the design and implementation of protection mechanisms were identified in Saltzer and Schroeder's influential "The Protection of Information in Computer Systems", (available at `http://www.cs.virginia.edu/ evans/cs551/saltzer/`). "Separation of privilege" and "least privilege" are two of the eight principles. How does RBAC relate to the other six principles?

Problem 3 This problem is based on the reading for Feb 17. A newer version of the paper, which explains some parts in more details, is available from the syllabus page.

a. (15 pts) Let $e_1 = \mathsf{ssod}\langle\{p_1, p_2, p_3, p_4\}, 3\rangle$, $PA_1 = \{(r_1, p_1), (r_1, p_4), (r_2, p_2), (r_2, p_4), (r_3, p_3), (r_4, p_4)\}$, $RH_1 = \emptyset$, $C = \{\mathsf{smer}\langle\{r_1, r_2\}, 2\rangle, \mathsf{smer}\langle\{r_1, r_3\}, 2\rangle, \mathsf{smer}\langle\{r_2, r_3\}, 2\rangle\}$. Give a SAT instance that is satisfiable if and only if C does *not* enforce $\{e_1\}$ under PA_1 and RH_1.

b. (5 pts) Given the following SSoD policy

$$e_2 = \mathsf{ssod}\langle\{p_1, p_2, p_3, p_4, p_5, p_6\}, 4\rangle$$
$$PA_2 = \{(r_1, p_1), (r_2, p_2), (r_3, p_3), (r_4, p_4), (r_5, p_5), (r_6, p_6)\}$$

Give one RSSoD requirement that is equivalent to $(\{e_2\}, PA_2)$.

c. (10 pts) Let $RH_2 = \{\}$. Find a set of SMER constraints that minimally enforces the above RSSoD requirement under PA_2 and RH_2.

d. (10 pts) Let RH_1 to be such that every pair of roles in $\{r_1, r_2, r_3, r_4\}$ have a parent role and these parent roles are all different, i.e., $RH_1 = \{r_7 \geq r_1, r_7 \geq r_2, r_8 \geq r_1, r_8 \geq r_3, r_9 \geq r_1, r_9 \geq r_4, r_{10} \geq r_2, r_{10} \geq r_3, r_{11} \geq r_2, r_{11} \geq r_4, r_{12} \geq r_3, r_{12} \geq r_4\}$. Find a set of SMER constraints that minimally enforces the above RSSoD requirement under PA_2 and RH_2.

Problem 4 (10 pts) Relate the safety analysis problem (the Harrison-Ruzzo-Ullman paper) in the context of RBAC. How would you define a similar problem in RBAC? What do you think are the most useful analysis problems in RBAC?

Problem 5 (10 pts) Exercise 2.1 in Nilsson and Maluszynski: *Logic, Programming and Prolog*. (Reading for Thursday Feb 24)

Problem 6 (10 pts) Exercise 2.2 in Nilsson and Maluszynski: *Logic, Programming and Prolog*. (Reading for Thursday Feb 24)

Problem 7 (10 pts) Exercise 2.5 in Nilsson and Maluszynski: *Logic, Programming and Prolog*. (Reading for Thursday Feb 24).