

Assignment #2

Due: Tuesday, September 27th, 2005.

Problem 1 (20 pts) The following questions are based on the following access control matrix:

	S_1	S_2	S_3	O_1	O_2	O_3
S_1				o,r,w,c		w,c
S_2				r	o,r	r
S_3				r	w,c	r,o

The following commands are the only ones defined for this system:

```
command grant_right( $p, f, q, r$ )
  if  $r$  in  $a[p, f]$  and  $c$  in  $a[p, f]$ 
  then
    enter  $r$  into  $a[q, f]$ ;
end
```

```
command delete_right( $p, f, q, r$ )
  if  $r$  in  $a[p, f]$  and  $o$  in  $a[p, f]$ 
  then
    delete  $r$  from  $a[q, f]$ ;
end
```

```
command grant_ownership( $p, f, q$ )
  if  $r, w, c, o$  in  $a[p, f]$  and  $r, w$  in  $a[q, f]$ 
  then
    enter  $o$  into  $a[q, f]$ ;
end
```

a What does the above access control matrix look like after the execution of the following sequence of commands. Please re-draw the matrix after each command and use the resultant matrix for the next subsequent command.

1. *grant_right*(S_1, O_2, S_3, r)
2. *grant_right*(S_2, O_2, S_3, r)
3. *grant_ownership*(S_2, O_2, S_3)
4. *grant_right*(S_1, O_1, S_3, w)
5. *grant_ownership*(S_1, O_1, S_3)
6. *delete_right*(S_3, O_1, S_1, w)

7. $delete_right(S_3, O_1, S_1, r)$
8. $grant_right(S_3, O_2, S_1, w)$
9. $grant_right(S_1, O_3, S_3, w)$
10. $grant_right(S_1, O_3, S_2, w)$
11. $grant_ownership(S_3, O_3, S_2)$

- b** Assume that if $w \notin a[S_2, O_k]$ where $k = 1, 2, 3$, then the system is secure. Is there a series of commands that will make the system insecure?
- c** Harrison, Ruzzo and Ullman proved in their paper “Protection in operating systems” in 1976 that “It is undecidable whether a given state of a given protection system is safe for a given right.”

The question posed in part b asks about a right, w ; why are you able to answer that question if the problem is undecidable?

Problem 2 (30 pts) Bell La-Padula Model:

- a** Given the security levels TOPSECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, say what type of access (read, append, write) is allowed according to the Bell-La Padula model in the following situations. Assume discretionary access controls allow anyone access unless otherwise specified.
1. Paul, cleared for (TOPSECRET, A, C), wants to access a document classified (SECRET, C).
 2. Anna, cleared for (CONFIDENTIAL, C), wants to access a document classified (CONFIDENTIAL, B).
 3. Jesse, cleared for (SECRET, C), wants to access a document classified (CONFIDENTIAL, C).
 4. Sammi, cleared for (TOPSECRET, A, C), wants to access a document classified (CONFIDENTIAL, A).
 5. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, B).
- b** One additional property of the Bell-La Padula model not discussed in class is the tranquility principle, which states that the classification of a subject or object does not change while it’s being referenced. Why is this principle necessary? What might happen in a system where this principle didn’t hold true?
- c** Given a DAC system describe how a MAC system could be “implemented” on top of this DAC system. Please discuss any problems and assumptions. For simplicity you can assume that the levels of the users are static and cannot change.

Problem 3 (25 pts) Read the paper “Quantum Cryptography” by Chip Elliott, and answer the following questions.

- a** Currently the method used for distributing a cryptographic key is to use an algorithm such as RSA or Diffie-Hellman. The quantum key distribution (QKD) method described in this paper effectively completes the same task as RSA or Diffie-Hellman. In your opinion, using specifics from the paper, will QKD replace the use of RSA or Diffie-Hellman in securely distributing keys? Focus on both the theoretical and practical limitations and advantages of both methods. (Keep your answer to 1 page in length.)

- b What is privacy amplification in QKD? Why is it needed in practical implementations of QKD, but not theoretical models?

Problem 4 (25 pts) Adaptive Access control:

The following paper gives an example and issues in adaptive access control:

Julien, C., Payton, J., and Roman, G.-C., "Adaptive Access Control in Coordination-Based Mobile Agent Systems," Software Engineering for Large-Scale Multi-Agent Systems III, R. Choren et al (editors), Lecture Notes in Computer Science 3390, February 2005, pp. 254-271.

[http : //www.ece.utexas.edu/ julien/pubs/selmas04LNCS.pdf](http://www.ece.utexas.edu/~julien/pubs/selmas04LNCS.pdf)

Discuss your notion of Adaptive Access Control system and compare it with the notion presented in the paper. Show the uses, possible ways to implement it and the corresponding problems of your notion of the adaptive access control. Clearly justify your claims.