

CS 461 / ECE 422 Information Assurance

HW #4

Due submitted to Compass by 3:30 p.m. March 13

- (1.5 points) Suppose your first job after graduating is for a start-up company that is developing a service which subscribers with cell phones that are GPS and web-enabled can purchase. The user logs into the service, the GPS coordinates are automatically reported, and the user can browse for shops and services in the near vicinity. Your job is to design the password system for this application. Outline the important considerations, identify your critical design decisions, and defend them.
- (2 points) Consider a system using the Bell-LaPadula model. Notation for clearance level is TS (top secret), S (secret), C (confidential), U (unclassified). Notation for categories is P (Peoria), C (Champaign), U (Urbana), D (Danville). Consider the table below with possible classifications:

(TS, {P})	(TS, {P,C})	(TS,{C,D})	(C,{P,C,U})
(S,{P,D})	(C,{P,C})	(S,{U,D})	(U,{U})
(C,{P,C,U,D})	(U,{P,D})	(U,{P})	(U,{C,U})

Give

- a classification that is the least upper bound of the first row;
 - (TS, {P, C, D, U})
- a classification that is the greatest lower bound of the fourth column;
 - (U,{U})
- a table that describes a lattice diagram for these. In this diagram an arc would be directed from classification A to classification B if $A \text{ dom } B$, and there is no other classification C with $A \text{ dom } C$ and $C \text{ dom } B$. The answer should be in the form of a table where there is one row for each classification, then a colon, followed with a list of classifications to which the row's leading classification directs an arc (i.e., it's immediate descendents in the lattice).

(TS, {P}); (U, {P})
(TS, (P,C)); (TS, {P}) (C, {P, C})
(TS, {C, D});
(C, {P, C, U}); (C, {P, C}) (U, {C, U})
(S, {P, D}); (U, {P, D})
(C, {P, C}); (U, {P})
(S, {U, D}); (U, {U})
(U, {U});
(C, {P, C, U, D}); (C, {P, C, U}) (U, {P, D})
(U, {P, D}); (U, {P})
(U, {P})

$(U, \{C, U\}); (U, \{U\})$

3. (1.5 points) Given integrity levels $I_1 < I_2 < I_3 < I_4$, and categories A,B,C, describe what access (choose from {read, write, read-write, none}), is allowed under the strict Biba integrity model for each subject – object pair below
- (Alice, $I_3, \{A,B,C\}$), (file1, $I_3, \{A,B\}$)
 - Read
 - (Bob, $I_4, \{A,B\}$), (file2, $I_1, \{A,B\}$)
 - Write
 - (Charley, $I_2, \{A\}$), (file3, $I_3, \{A,B,C\}$)
 - None
4. (1.5 points) Imagine a security model with “access” levels. $A(s)$ gives the access of subject s , and $A(o)$ gives the access of object o . For every subject or object x , $A(x)$ is always between 0 and 1, exclusive. Each subject-object pair is categorized as being either “independent”, or “dependent”. The system operates under the following rules :
- Subject s and read from or write to object o only if $A(s) \leq A(o)$.
 - When subject s reads object o with which it is independent, the access of s changes to $A(s)*A(o)$, i.e., the product of the access of s and o .
 - When subject s reads object o with which it is dependent, then after s reads o , the access of s changes to the average $(A(s)+A(o))/2$.
 - When s writes to an object o with which it is dependent, then $A(o)$ becomes $A(s)$.
 - When s writes to an object o with which it is independent, then $A(o)$ does not change.
 - Subject s is unable to read or write any object if $A(s) = 0$, and object o cannot be read from or written to when $A(o) = 0$.

Prove that if in the initial state $A(s) > 0$ and $A(o) > 0$ for all subjects s and objects o , then the same is true in every state of the system regardless of the number or nature of the read/write transitions.

Proof: By induction on the number of transitions: among all read/write transition rules, no rule will lead any object or subject's access level to 0

5. (2 points) In the same access model as described in problem 4, show by example that it is possible to have an initial state where subject s is able to read and write to object o , but that a sequence of system transformations exist that bring the system to a state where s cannot read o .

Suppose there are one subject and two objects:

$$A(S) = 0.1$$

$$A(O_1) = 0.2$$

$$A(O_2) = 0.7$$

S and O_1 are independent while S and O_2 are dependent.

Observe that S can read O_1 and O_2 in the initial state. After S reads O_2 . Then $O(S) = (0.1 + 0.7)/2 = 0.4$ then $A(S) > A(O_1)$, S cannot read O_1 anymore.

6. (1.5 points) In the same access model as described in problem 4, show that if all subjects are independent of all objects, then information transfer path exists to a state such that every subject can read every object.

Proof: suppose there are m subjects, n objects, without loss of generality, all subjects are represented by s_i , where $1 \leq i \leq m$ and $A(s_i) \leq A(s_j)$ for $1 \leq i \leq j \leq m$; all objects are represented by o_i , where $1 \leq i \leq n$ and $A(o_i) \leq A(o_j)$ for $1 \leq i \leq j \leq n$. According to the assumption, $A(s_m) \leq A(o_n)$, i.e. for any subject s_i , it can read/write at least one object. Suppose any subject s_i can read/write an object o_j while cannot read/write o_k where $k < j$. Because all subjects are independent of all objects, if s_i can read o_j , then $A(s_i) = A(s_i) * A(o_j)$. Because $0 < A(s_i) \leq A(o_j) < 1$, we know the new $A(s_i)$ must be less than the old one. Thus, by reading o_j for a certain times, $A(s_i)$ could be less than any number just greater than 0, thus s_i can read any object.