The University of Western Ontario
London Canada

Department of Computer Science

Computer Science 9616a – Database Security

Take-home Test, Part 2

Due: Nov. 25, 2015 at 3:30 p.m.

Please write or type neatly!

You are expected to work alone on these questions.

1. (DAC for Objects) (10 marks) These questions relate to the AOG below for an object-oriented database. Items in quotation marks, x3456, and 1985/12/30 refer to atomic values. All other nodes in the graph not labelled System, Database or Class, refer to objects. The access modes are CREATE, UPDATE and READ, and the ATG has edges CREATE → READ and UPDATE → READ. Assume that Employee objects have attributes: firstName, lastName, dateOfBirth, Department, Projects (which is a set-valued attribute). Assume Departments and Projects have a name attribute, and others which are not shown.

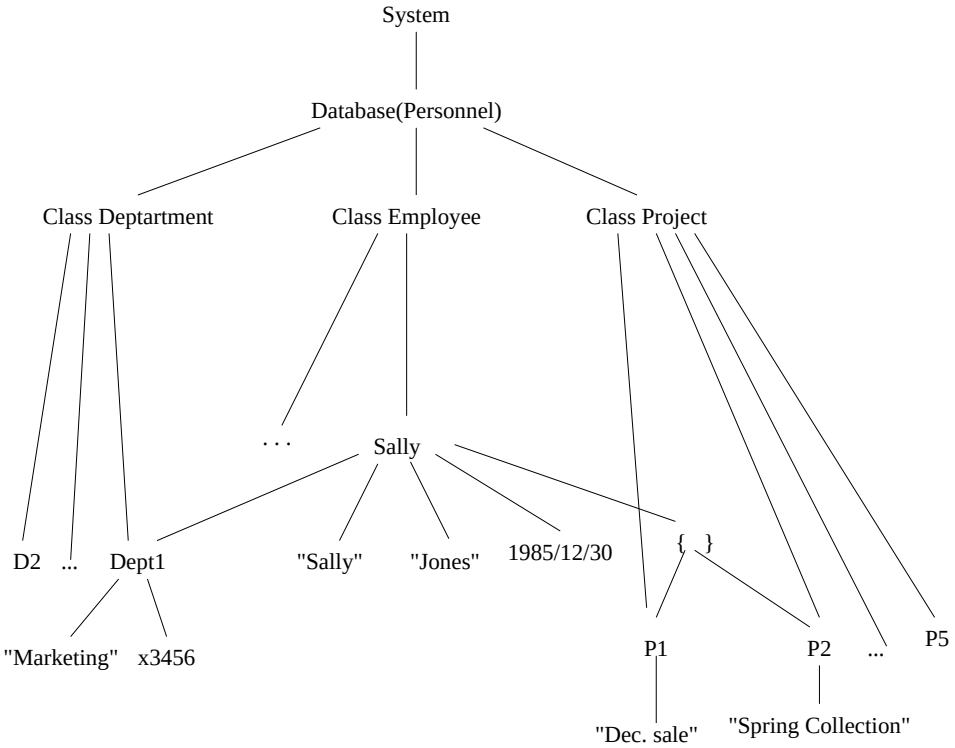
   (a) Given all the nodes in the AOG, for what nodes does it make sense to apply the CREATE access mode?

   (b) We want Alice to be able to read all the information about Sally, except for her date of birth and projects. What strong or weak authorizations will allow that?

   (c) Specify the strong/weak authorizations that would allow Alice to read all firstNames and lastNames of all employees.

   (d) If I grant Bob a weak, positive, UPDATE authorization on object Sally, what are all the implications of this? I.e. list all the operations can Bob do on what data.

   (e) Specify the authorization(s) that would allow Carol to update all the information about Projects, without being able to read anything else.



2. (MAC for objects) (12 marks)

This question assumes the Sorion model. Suppose we have a class definition for Employee, which has attributes:

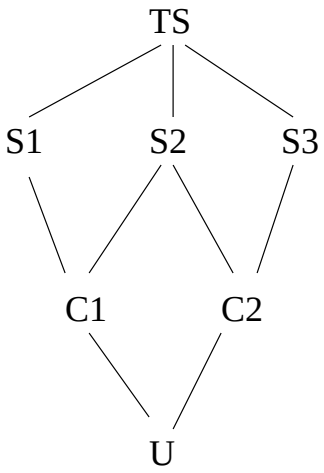
Ename : string

Enumber : integer

Edept : Department

EManager : Employee

where Department is another class in the database, and string and integer are base types. Suppose we have security levels arranged in a lattice as shown here:



(a) If class Department is labeled C2, what is the lowest label that can be attached to the class definition for Employee? Justify your answer.

(b) Given your answer to (a), what security level(s) can be attached to the attribute names in class Employee? Justify your answer.

(c) If the class definition for class Employee is classified according to your answer to (a), can we have Employee instances at level U? C1? C2? S1? S2? S3? or TS? Justify your answer.

(d) Again, if the class definition for class Employee is classified according to your answer to (a), suppose we have an Employee instance E1, with Ename "Robert", Enumber value 12345, Edept value equal to object D1, and Emanager equal to E2. D1 is at level C2.

i. what is the level of value "Robert"? Justify your answer.

ii. Is it possible for E2 to be classified S1? Justify your answer.

iii. Is it possible for E2 to be classified TS? Justify your answer.

3. (Statistical Databases) (10 marks)

Consider the following data (disclaimer: these data are not guaranteed to be accurate):

Faculty	Name	NoOfCh	Rank	Sex	Salary
	Barron	2	Full	M	220
	Bauer	2	Full	M	330
	Beauchemin	0	Assoc	M	120
	Boykov	2	Assoc	M	240
	El-Sakka	2	Assoc	M	130
	Ilie	1	Full	M	250
	Jurgensen	2	Full	M	310
	Katchabaw	2	Assoc	M	140
	Lazotte	0	Asst	M	100
	Ling	2	Full	M	230
	Lutfiyya	0	Full	F	260
	Madhavji	2	Full	M	150
	Maguilli	0	Limited	M	100
	Mercer	2	Full	M	270
	Moreno Maza	0	Assoc	M	160
	Osborn	2	Assoc	F	400
	Reid	2	Limited	F	280
	Sedig	2	Assoc	M	170
	Solis-Oba	3	Assoc	M	180
	Veksler	2	Assoc	F	201
	Webber	0	Assoc	M	203
	Zhang	1	Full	M	204

These can be summarized as follows:

Rank	Sex	NoOfCh			
		0	1	2	3
Limited	M	1	0	0	0
	F	0	0	1	0
Assist	M	1	0	0	0
	F	0	0	0	0
Assoc	M	3	0	4	1
	F	0	0	2	0
Full	M	0	2	5	0
	F	1	0	0	0

The salary attribute is one for which we wish to restrict statistical queries so that individual salaries cannot be revealed.

(a) Let us define as *vulnerable* any faculty member who falls into a set of size 1, when the attributes NoOfCh, Rank and Sex are used. Who is vulnerable in this database?

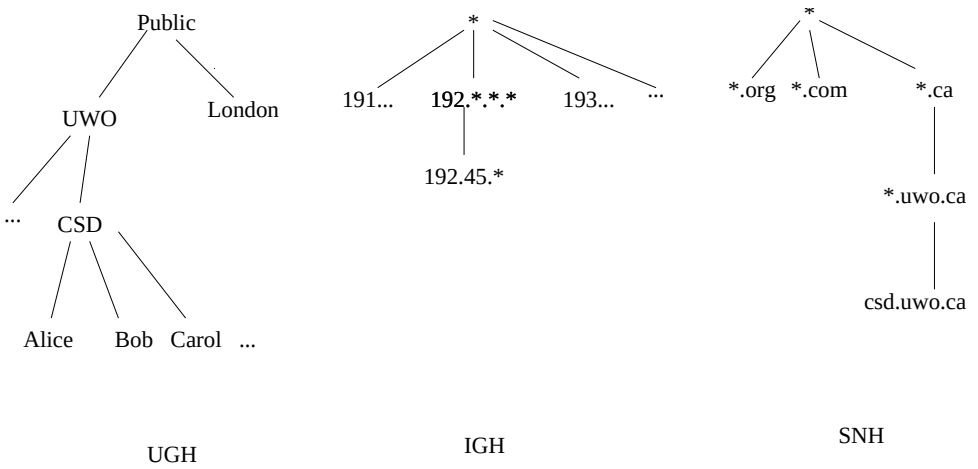
(b) Pick one of the vulnerable professors, and give a characteristic formula which describes this professor.

(c) Give a **general** tracker for this data. Show how the tracker is used for compromizing the data, by showing the actual queries and their results to find the salary of the professor you picked in part b.

4. (XML) (8 marks)

This question relates to the material from the paper by Damiani, et al. starting on page 61, Set 7 of the notes. There is an xml file for the Shakespearean play, Hamlet, available at http://www.csd.uwo.ca/courses/CS9616a/hamlet.xml. We will refer to it below simply as hamlet.

The following is the Authorization Subject Hierarchy you are to use:



The following permissions have been granted (assume the syntax is correct):

P1: <(CSD, 192.45.*, csd.uwo.ca), hamlet://SPEECH, read, +, R>

P2: <(Bob, 192.45.*, csd.uwo.ca), hamlet://SPEECH[contains(SPEAKER, 'HORATIO')]/LINE, read, -, L>

(a) What data can Alice read?

(b) What data can Bob read?

(c) We want Carol to be able to read all SPEECHs in the document, but not the SPEAKERs. What permission(s) are necessary? You can reuse, revoke or ignore P1 and P2 if you wish.

5. (Privacy) (10 marks)

(a) Summary data for the faculty relation is given on page 4 of this takehome. I am sharing this data with you for the 9616 takehome, but the takehome is visible on the course web page. Discuss where this summary data fits in the Barker et al. taxonomy. Explain your choice for each axis of the taxonomy.

(b) Of the 10 principles listed in the Hippocratic Databases paper, pick one whose implementation could be considered a "normal database" issue to comply with, and one which is "privacy related". Discuss briefly your reasons for your choices.