IS2510/TEL2810 Information Security & Privacy

Homework 2

Total Points: 100

Due Date: Monday, March 4, 2013

1. **[30 Points]**

   (a) Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

   a. Jesse, cleared for (SECRET, {C}), wants to access a document classified (CONFIDENTIAL, {C}).
   b. Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}).
   c. Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (CONFIDENTIAL, {B }).

   (b) Suppose a system implementing Biba's model used the same labels for integrity levels and categories as for security levels and categories. Under what conditions could one subject read an object? Write to an object?

   (c) In the DG/UX system, (i) why is the virus prevention region *below* the user region and (ii) the administrative region is above the user region?

2. Do the following from Section 8.7 (Green Book): Exercise 11, 12, 17 **(Points 30)**

3. **[40 Points]**
   Suppose the following medical record dataset has been published.

SSN	Name	Race	DateOfBirth	Sex	ZIP	Marital Status	HealthProblem
		asian	09/27/64	female	94139	divorced	hypertension
		asian	09/30/64	female	94139	divorced	obesity
		asian	04/18/64	male	94139	married	chest pain
		asian	04/15/64	male	94139	married	obesity
		black	03/13/63	male	94138	married	hypertension
		black	03/18/63	male	94138	married	shortness of breath
		black	09/13/64	female	94141	married	shortness of breath
		black	09/07/64	female	94141	married	obesity
		white	05/14/61	male	94138	single	chest pain
		white	05/08/61	male	94138	single	obesity
		white	09/15/61	female	94142	widow	shortness of breath

Considering the publicly available voter registration list below, answer the following questions.

Name	Address	City	ZIP	DOB	Sex	Party	.....
.....	.....	.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....	.....	.....
Sue J. Carlson	900 Market St.	San Francisco	*94142*	*9/15/61*	*female*	democrat	.....
.....	.....	.....	.....	.....	.....	.....	.....

a. Answer the following questions:
    i. What kind of anonymization has been performed on the released dataset before being published, if any?
    ii. Explain if it is possible to infer any privacy-sensitive information from the released data using the voter list.

b. Consider the medical record dataset above. Given attributes *Race*, *DOB*, and *Sex* together as the quasi-identifier, and attribute *Health Problem* as the sensitive attribute, create and report a 2-anonymous version of the medical dataset (*k*-anonymity where *k=2*). How many equivalency classes are there in the result dataset?

   Note: There is no unique answer to this question. However, your result should have fairly low information loss.

c. Repeat the previous exercise for attributes *Sex*, *ZIP*, and *Marital Status* as quasi-identifier with $k = 3$. Explain what the *l* value of the result is in terms of the *l*-diversity principle (considering distinct *l*-diversity)?

d. Suppose a social network graph of a Facebook-like system has been released. The dataset is simply a list of links among pairs of nodes in the network, and some attributes about the nodes. Explain if there is any privacy risk with this practice?