Homework 2 Database Security

Short answers

1. A user is cleared for <secret>. Can he have access to data objects labeled <classified>? Why?

Yes. According to the *Simple property* of the BLP model, read-down is allowed.

2. The user at <secret> level wants to pass a file to a user at <top secret> level, how could he do that?

A top-secret user could naturally read files from lower security levels. The <secret> level user does not need to do anything.

3. Multi-level security is used in a database system. Access control is enforced at record level, which means there is no attribute-level classification. The following table contains records about employees' information:

UID	title	task ID	report date	TC
72564	manager	K2398	09/20/2015	S
35920	special agent	D9372	08/28/2015	C
56973	special agent	K8364	09/05/2015	UC
00369	director	K2398	09/27/2015	TS
65851	assistant	K2934	09/20/2015	S

3.1 A user at security level 'S' browses the database, what could he/she see from the table?

UID	title	task ID	report date	TC
72564	manager	K2398	09/20/2015	S
35920	special agent	D9372	08/28/2015	C
56973	special agent	K8364	09/05/2015	UC
65851	assistant	K2934	09/20/2015	S

3.2 A user at security level 'TS' wants to add a task for UID 65851 with the following information: (65851, assistant, M9374, 12/21/2015). How will the request be processed (show the updated table)? What is the rationale behind the procedure?

UID 65851 already exists, and its security level is S. When a TS level user changes the record, we cannot simply update the data and change its Tuple Classification to TS, since it will give S level users a hint that the record has been updated by a high-level user.

UID	title	task ID	report date	TC
72564	manager	K2398	09/20/2015	S
35920	special agent	D9372	08/28/2015	C
56973	special agent	K8364	09/05/2015	UC
00369	director	K2398	09/27/2015	TS
65851	assistant	K2934	09/20/2015	S
65851	assistant	M9374	12/21/2015	TS