Computer Security
Dr. Simon Foley
MAC Problem Set

Department of Computer Science,
University College,
Cork, Ireland.

1. A simple multilevel secure database management system is to be designed. Each tuple in a database table is assigned a separate security-level, and subjects at any security-level may access the table (but not necessarily every record in the table). For example, consider the following employee relation table (*emp-id* is primary key).

emp-id	*level*	Name
0031	topsecret	Mulder
0200	secret	Scully
1002	secret	Jones

   Given the usual ordering between the specified security levels, a secret process may read the Scully and Jones' entries but not the Mulder entry, and so forth.

   (a) Propose suitable multilevel security rules that govern read/write access by subjects to table rows. You should assume that when a new tuple is inserted into the table it is assigned the security-level of the subject inserting it.

   (b) Given that primary key values are unique in a table, explain how a Trojan-Horse running at top-secret could establish a covert-channel and signal one bit of information to a subject operating at secret. (Hint: recall the multilevel file-system discussed in lectures). Suggest how the covert channel might be closed.

2. A networked server hosts a Kerberos Authentication Service and an Apache web-server that uses a MySQL back-end database server. A buffer overflow vulnerability was discovered in the application running with the Apache server and there are concerns that other (unknown) vulnerabilities may exist in the application system. Discuss the impact of this vulnerability.

   It has been decided to replace the existing server host by a high-assurance system that enforces mandatory Multilevel security (MLS). Describe the (Bell LaPadula) access-rules for MLS and give a suitable compartmentalization policy for the server host that would provide better system protection. Discuss any limitations of this approach.

3. A multilevel secure system has only one printer which is used to print jobs at all security levels. It is in a secured area and printouts are carefully labelled. A multilevel secure (trusted) print queue manager accepts requests from subjects at any security level. Its operations are:

   (a) `lpr <filename>`. Assign job number and add file to print queue. Returns `job#` to requester.

   (b) `lprm <job#>`. Remove specified print job. Returns `success` or `failure`.

   Sketch suitable algorithms that describe the behaviour of the above operations taking care to ensure that multilevel security is preserved. For the sake of simplicity it is not necessary to consider printer controls/scheduling.

4. Describe how a system supporting a Type Enforcement mandatory access control model might help safeguard against possible buffer overflows in applications such as web-browsers. Your answer should include a suitable Domain Definition Table.

5. A multilevel secure system that implements the Bell LaPadula model is configured with a partial ordering based on compartments sales, admin and stock. Most applications run as untrusted, except for a special trusted program Stats that is used to generate statistics from sales data and copy it to personnel files in the admin compartment.

   (a) Give a diagram that specifies the partial order based on these compartments.

   (b) What is the difference between a *trusted* and *untrusted* subject? Why is it necessary to treat Stats as trusted?

   (c) Outline how a Type Enforcement mechanism can enforce the above multilevel security requirement. Explain why the Type Enforcement approach provides better support for the Principle of Least Privilege than the Bell LaPadula model.

6. Devise a suitable partial order and user-bindings for the information flow policy outlined below:

   A hospital has the following types of user: *doctor*, *nurse*, *manager* and *clerk*. A computer system is used to store information about treatments (prepared by nurses for patients), medical history (maintained by doctors), and financial accounts (which are prepared by clerks).

   For confidentiality reasons only doctors may read patient medical history. For profitability reasons, only managers and clerks may access financial accounts.

   Mangers coordinate information: they forward treatment details to doctors, and combine treatment details and financial accounts to generate bills for patients.

7. Suppose that we introduced a conflict of interest style constraint to the policy in Question 6 above which required that a manager who accesses financial information may no longer access treatment information, and vice-versa. Outline the changes to the mechanism and policy that would be necessary to support this constraint.

8. A multilevel secure system offers a document indexing system with the operations:

   - assign(n,p,s): give the document (file) located at path p the name n.
   - view(n,s): view the contents of the document with name n.

   where s is the subject requesting the operation. Note that document names are unique across the system and are in addition to the name (path) given to the file containing the document. A table is used to store the name-path relationship, for example:

Name	Path
ExamPaper	/home/store/a
Attendance	/home/store/b
LectureNotes	/home/store/c

   Sketch suitable algorithms that describe the behavior of the above operations taking care to ensure that multilevel security is preserved.

Simon Foley, February 2, 2016