Question 2

The back-end DBMS of a retail web-site www.amadan.com stores customer order details in a database table CUST which includes attributes OrderID, UserID, NameAddress, CreditCard.

a) Prior to placing an order a customer logs in by providing their userID and password. If successful, they are directed to a URL that includes a simple authenticator, for example,

http://www.amadan.com/order.asp?p1=simon&p2=12345

whereby the user simon need not re-authenticate so long as he includes p2=12345 in any URL. The authenticator is a simple global sequence number, incremented on each login. Describe an attack on this scheme whereby an attacker can masquerade as another user. Outline how the attack can be avoided by using authenticator cookies. (15 marks)

c) The website owners have a choice of deploying the web-server plus DBMS on either a standard Linux server or on an SELinux server that provides Type Enforcement based access control. Advise the website owners on the choice and illustrate your answer by comparing a Linux user-group policy versus a Domain Definition Table. (15 marks)

Linux user-group policy

Domain Definition Table

A Domain Definition Table (DDT) defines the allowable access rights within a domain. A DDT provides fine grained control by allocating different types to different domains. Here each domain has limits on the privileges allowed to each of the different types, and no other domain is accessible from within a particular domain ie. if a domain is compromised, there is limits on the amount of damage an attacker can do.

Question 4

a) Write a note on computer viruses, considering their operation and infection. Discuss the effectiveness of the following techniques in defending against viruses: virus checkers, code-signing, security-kernels. (15 marks)

b) 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:

i. lpr <filename>. Assign job number and add file to print queue. Returns job# to requester.
ii. 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. (15 marks)

- Answered in Mac Exercises