

IY5512: Coursework 7a:

Worked solutions

1. *MD5 has replaced a modified version of DES for use in password protection in more recent versions of Unix. Does this make any significant difference to the security of the user authentication system? Explain your answer.*

Replacing DES with MD5 does not appear to have made a huge difference to the security of Unix password protection. Since DES was used as a one-way function, and since its operation was salted, the weakness of DES as an encryption function does not appear to have been a major vulnerability.

The main improvement in security of Unix passwords has been to move the protected passwords into the shadow file, so that they are not world readable. That is, the major weakness of the old system was that the publicly available file of protected passwords could be used as the basis of a brute-force password search. The choice of the cryptographic function (DES, MD5 or anything else for that matter) makes no difference whatever to the possibility of performing such a search.

Because of the change in the way the protected passwords are stored, brute force password searches are no longer possible, except (of course) for system administrators.

2. *Describe (briefly) how the Unix access control system operates. Indicate in your description which types of file operations are controlled via directories.*

In the Unix operating system, access control policies are expressed in terms of three operations: read (reading from file), write (writing to a file), and execute (executing a file). These operations differ from the access rights of the Bell-LaPadula model. For example, in Unix, write access does not include read access. There is no explicit notion of a delete operation (which is present in some other operating systems). Control of file deletion (and file creation) is handled in Unix by controlling access to directories in the same way as to files.

Access rights (from read, write and execute) are assigned to three classes of subjects: user (owner), group and other. The *mode* of a file determines which users are permitted the various types of access. The owner of a file (or the root superuser) can always change the mode of a file, even if the mode denies access to the file for the owner (which is perfectly possible).

Permissions apply to the most specific categorisation of the user requesting access. If the user is the owner of the file, then the Owner permissions only are applied. Otherwise, if the user is a member of the file's group, then the Group permissions are applied. Otherwise the Other permissions are applied.