CprE 431
Homework 3

Sean Gordon

Sep 20, 2020

1. DAC

   - Access is determined using the user's identity and ACE entries.
   - A user is given access to a file by being added to its ACL.
   - A user can extend permissions it has to other users.

   MAC

   - Access is determined using a user's role.
   - Access is given ONLY by administrators.

2. Salt is used simply to change the hash. This stops an attacker from breaking hashes by just generating a single list of hashes for common passwords. An attacker will now need to generate that list for each salt value as well.

3. (a) High security, but have to change permissions for each file to share with a broader audience.
   Best for a system where files are considered important unless stated otherwise, like a government org.

   (b) Security based on groups, less secure but easier to work with.
   Best for a set of groups which kep their work private from each other, but top security is not necessary, like a large business.

   (c) Low security, but very easy to work with.
   Best where every user is trusted and works closely together, like a small business.

4. (a) Each running service takes computer resources, and could be available for use to an attacker.
   (b) Information is stored in the /etc directory or the installation tree for specific applications.
   (c) It is used to restrict a users view by mapping root to another location, essentially trapping them in that directory and its children. It is fairly easy to escape however, with many documented mechanisms.

5. (a) Allows system administators to more quickly identify any issues.
   (b) Can only tell you what has already happened, and only at certain ranges of data.
   (c) Remote logging doesn't require logs to be kept on the system they are created. However, it takes bandwith.
   (d) If log files are not rotated, they stay forever and quickly build up space.

6. (a) User tries multiple times to log in with different passwords.
   (b) User tries accessing unusual websites that have been flagged as malicious.