Password Storage Concepts

- Salting:
- A salt is a unique, randomly generated string that is added to each password as part of the hashing process.
- As the salt is unique for every user, an attacker has to crack hashes one at a time using the respective salt rather than calculating a hash once and comparing it against every stored hash.
- This makes cracking large numbers of hashes significantly harder, as the time required grows in direct proportion to the number of hashes.

Password Storage Concepts

- Salting also protects against an attacker pre-computing hashes using rainbow tables or database-based lookups.
- Finally, salting means that it is impossible to determine whether two users have the same password without cracking the hashes, as the different salts will result in different hashes even if the passwords are the same.
- Modern hashing algorithms such as Argon2id, bcrypt, and PBKDF2 automatically salt the passwords, so no additional steps are required when using them.

Password Hashing Algorithms

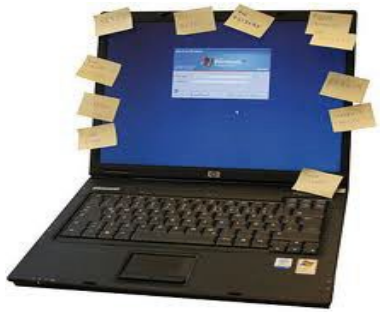
- There are a number of modern hashing algorithms that have been specifically designed for securely storing passwords. This means that they should be slow (unlike crypto hashes such as SHA family & KECCAK, which were designed to be fast), and how slow they are can be configured by changing the work factor.

- Argon2 is the winner of the 2015 Password Hashing Competition.
- The bcrypt password hashing function should be the second choice for password storage if Argon2 is not available

PASSWORD SECURITY

Is security highest if users are forced to use long passwords, mixing upper and lower case characters and numerical symbols, generated for them by the system, and changed repeatedly?

1. Users may have difficulty memorizing complex passwords.
2. Users may have difficulty dealing with frequent password changes.
3. Users may find ways of re-using their favourite password.



Passwords will be written on a piece of paper kept close to the computer

Is it always a bad idea to write down your password?

PASSWORD POLICIES - Recap

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

1

Set a password

If there is no password for a user account, the attacker does not even have to guess it.

2

Change default passwords

Often passwords for system account have a default value like “manager”.

- Default passwords help field engineers installing the system; if left unchanged, it is easy for an attacker to break in.
- Would it then be better to do without default passwords?

3

Avoid guessable passwords

- Prescribe a minimal password length.
- Password format: mix upper and lower case (case-sensitive), include numerical and other non-alphabetical symbols (alphanumeric).
- Today on-line dictionaries for almost every language exist.

PASSWORD POLICIES

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

4

Password ageing

- Set an expiry dates for passwords to force users to change passwords regularly.
- Prevent users from reverting to old passwords, e.g. keep a list of the last “ten” passwords used.

5

Limit login attempts

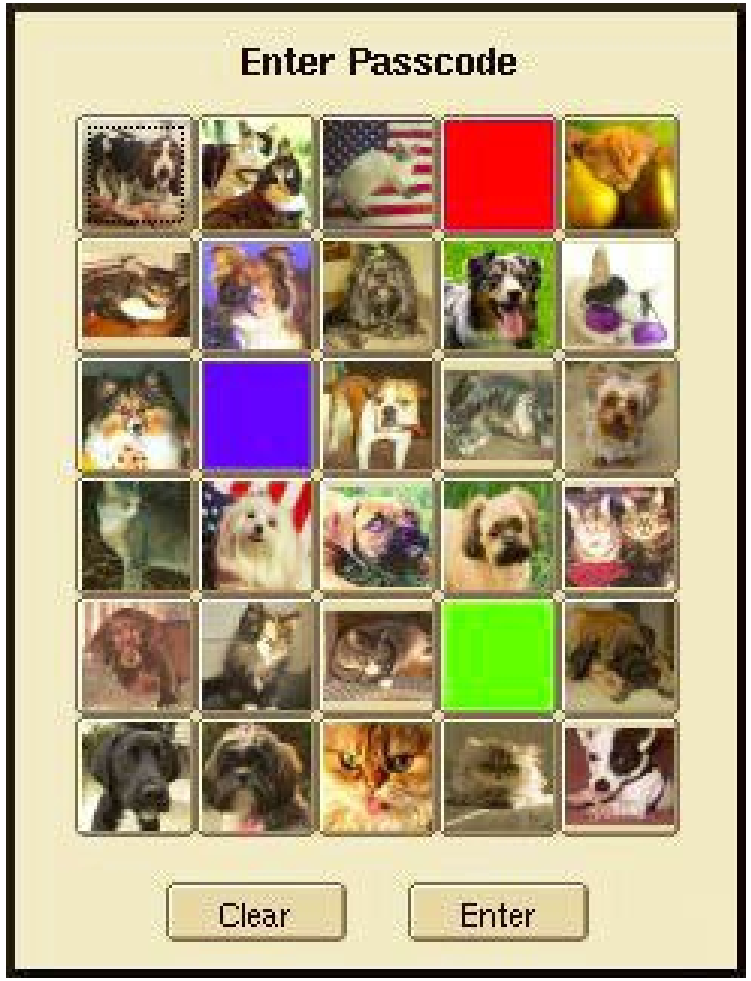
The system can monitor unsuccessful login attempts and react by locking the user account (completely or for a given time interval) to prevent or discourage further attempts.

6

Inform user

After successful login, display time of last login and the number of failed login attempts since, to warn the user about recently attempted attacks.

ALTERNATIVE FORMS OF PASSWORD



1 Passphrase

User enters sentences or long phrases that are easy to remember, and the system applies a hash function to compute the (fixed-size) actual passwords.

2 Visual drawing patterns

(on touch interface), used in, e.g. Android.

3 Picture passwords

Select objects in pictures and patterns. Used in Windows 8.

4 One-time passwords.

PROTECTING THE PASSWORD FILE

Password File

Operating system maintains a file with user names and passwords

Attacker could try to compromise the confidentiality or integrity of this password file.

- Options for protecting the password file:
  - cryptographic protection,
  - access control enforced by the operating system,
  - combination of cryptographic protection and access control, possibly with further measures to slow down dictionary attacks.