**Chapter 2**

Authentication is the binding of an identity to a subject.

A user or entity is often required to authenticate itself to a computer system.

e.g. Internet banking needs to be authenticated by the bank site.

False Acceptance rate (FAR)

* This will be the proportion of authentication attempts resulting in false acceptances.

False Rejection Rate (FRR)

* This will be the proportion of authentication attempts resulting in false rejections.

Password Authentication:

User supplies an identity.

User supplies a password.

* This is not necessarily what is sent to the “server”, that may be some function of the password.

Server checks the suppled information.

If the password information is associated with the user, the user’s identity is authenticated; otherwise, the password is rejected.

Threats against password systems

* Password guessing
* Password exposure
* Trojan login programs
* Poor passwords
* Common attacks:
  + Dictionary attacks
  + Brute force attacks
  + Hybrid attacks
* Online or offline
  + Compromise of the password file.

**Password entropy**

Entropy is to do with the information content, and randomness, and uncertainty.

* In this context the uncertainty of someone else regarding your password is a helpful way to think

Entropy is often measured in bits.

If there are two equally likely options, we have 1 bit of entropy, four equally likely options we have 2 bits of entropy and so on

The entropy for N equally likely options is log2N

**Protective mechanisms**

Keep track of incorrect password attempts:

* Limited the number of account/passwords guesses per connect attempt.
* Lock the account when a threshold is exceeded
  + Although the attacker can use this to perform a DOS attack.
* Raise an alarm and try to trace the intruder

Slowly process passwords, it doesn’t make much difference to a legitimate user, but it makes a lot to the processing speed of an attacker.

Determine the entropy associated with the following method of generating a password

**Hybrid attacks**

The hybrid attacks fall between the dictionary and the brute force attack, in the time consumed the number of passwords tried, and, therefore, in the (naïve) chance of success.

**Rules for password systems**

These are examples of rules, the application and details should be context dependent.

* Change passwords every 45 days.
* Min length of 8 or higher characters.
* Must contain at least 1 alpha, 1 number and 1 special character
* Alphanumerical and special characters should be mixed up
  + E.g. fg#g3s^hs5gw is good, abdheus#7 is not.
* Cannot contain dictionary words
* Cannot reuse previous 5 passwords.
* After 5 failed logon attempts, password is locked for several hours.