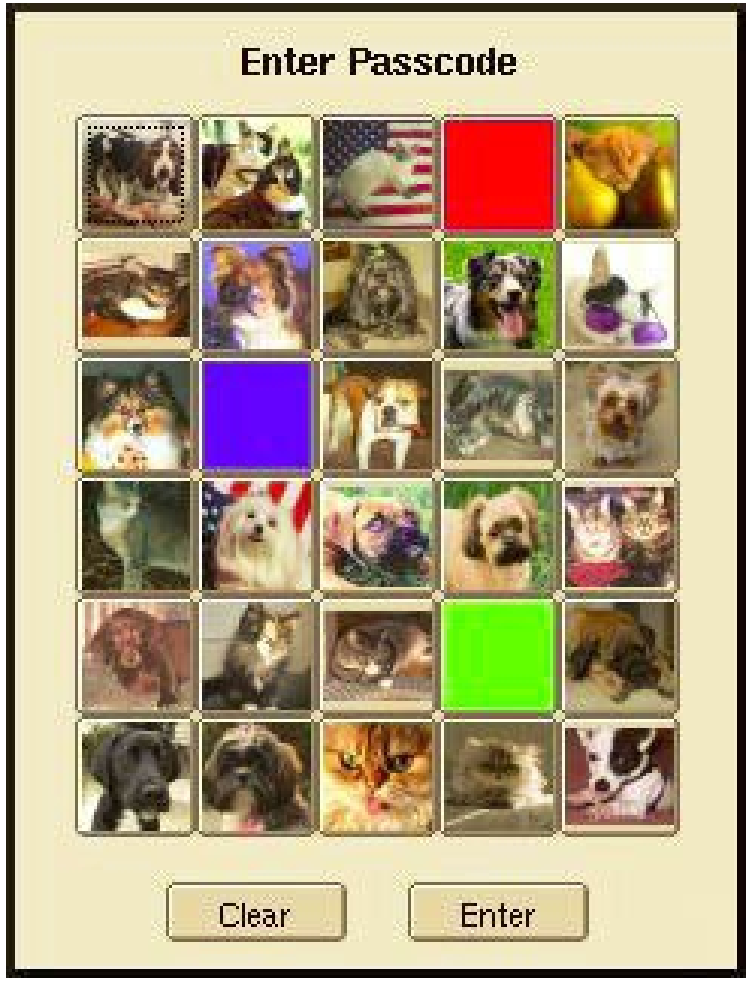
ALTERNATIVE FORMS OF PASSWORD



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.

ACCESS CONTROL SETTINGS

1. Only privileged users must have write access to the password file.
   - Otherwise, an attacker could get access to the data of other users simply by changing their password, even if it is protected by cryptographic means.

2. If read access is restricted to privileged users, then passwords in theory could be stored unencrypted.

3. If password file contains data required by unprivileged users, passwords must be “encrypted”; such a file can still be used in dictionary attacks.
   - Thus modern Unix/Linux system hides the actual password file in /etc/shadow that is not accessible to non-privileged users.

FAILURE RATES

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

1. Measure similarity between reference features and current features.
2. User is accepted if match is above a predefined threshold.

NEW ISSUE

False Positive

Accept wrong user: security problem.

False Negative

Reject legitimate user: creates embarrassment and an inefficient work environment.

FORGED FINGERS - Recap

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Fingerprints and Biometric Traits	Rubber Fingers	Secure Storage
In general, may be unique but they are no secrets. • In September 2013, hackers show how to lift fingerprints from iPhone 5s. Similar attacks also apply to Samsung S5 phone. http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid	Rubber fingers have defeated many commercial fingerprint recognition systems in the past. • Minor issue if authentication takes place in the presence of security personnel. • When authenticating remote users additional precautions have to be taken to counteract this type of fraud.	Secure storage of biometric data is an important requirement from the angle of personal privacy protection.

REFERENCES

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Suggested further reading on authentication (not mandatory):

- Menezes et al. *Handbook of Applied Cryptography*. Chapter 10. http://cacr.uwaterloo.ca/hac/

- R. Anderson. Security Engineering. Chapter 15. https://www.cl.cam.ac.uk/~rja14/book.html
- 2nd edition free & downloadable