OUTLINE

1. Basis of authentication:
   - what you know, what you possess, what you are.
2. Password-related techniques
3. Attacks on passwords and defense mechanisms
4. Authentication tokens and biometrics

AUTHENTICATION PROTOCOL

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

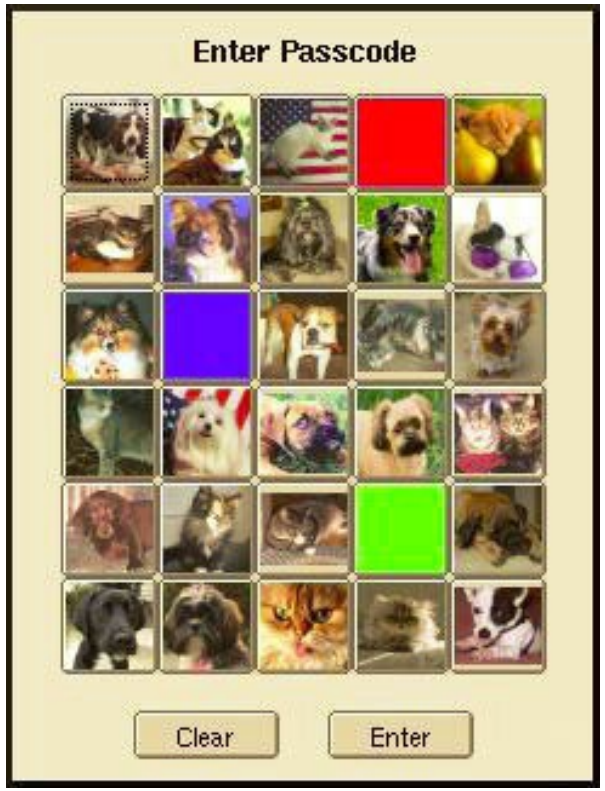
Weak/Simple Authentication:

- Password-based.
- Unilateral: one entity (claimant) proves its identity to the verifier.
- Prove knowledge of secret by giving up the secret

Strong Authentication:

- Involves mutual authentication; both parties take both the roles of claimant and verifier:
- Challenge-response protocols: sequence of steps to prove knowledge of shared secrets.
- Prove knowledge of secret WITHOUT giving up the secret (zero knowledge proofs)

PASSWORD-RELATED TECHNIQUES



- **Password storage:**
  - **Plaintext (BAD)** or **"encrypted" (fair)** or **"hashed" (good).**
- **Password policies:**
  - What rules need to be imposed on the selection of passwords by users, number of failed attempts, etc.
- **"Salting" of passwords.**
- **Alternative forms of passwords**
  - Passphrases, one-time passwords, visual passwords.

Salt is random data that is used as an additional input to a one-way function that "hashes" a password. Salts are used to safeguard passwords in storage. The primary function of salts is to defend against dictionary attacks.

ONE WAY FUNCTIONS

Password storage security relies on a cryptographic construct called ***one-way function***

A one-way function f is a function that is relatively easy to compute but hard to reverse.

- Given an input x it is easy to compute $f(x)$, but given an output y it is hard to find x so that $y = f(x)$

Hash functions are an example of one-way function:

- A hash function f takes an input x of *arbitrary length*, and produces an output $f(x)$ of *fixed length*.

PROPERTIES OF HASH FUNCTIONS

Suppose *H* is a hash function. We say *H* satisfies:

- *Pre-image resistant* if given a hash value y, it is computationally infeasible to find x such that $H(x) = y$.
- *Collision resistant* if it is computationally infeasible to find a pair (x, y) such that $x \neq y$ and $H(x) = H(y)$.

Recap: A one-way function f is a function that is very easy to compute but hard to reverse. Hash function is an example of one-way function. Impt Hash Functions: : **SHA256,512,KECCAK (crypto)** ,ARGON2,bcrypt (for password hashing)