Ecole Supérieure d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

# Introduction a la sécurité des systèmes d'information
# Authentication

**PRÉPARÉ PAR:**
**SEBBAR ANASS**

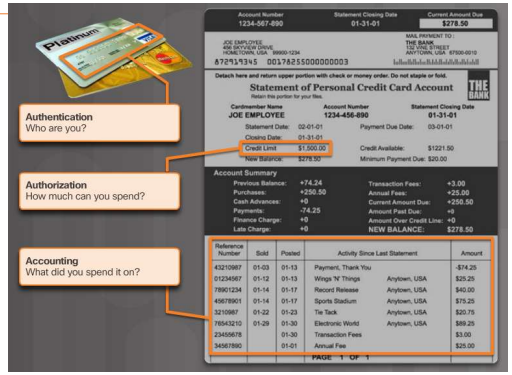
Année universitaire: 2022-2023

## User Authentication

- fundamental security building block
  - basis of access control & user accountability
- is the process of verifying an identity claimed by or for a system entity
- has two steps:
  - identification - specify identifier
  - verification - bind entity (person) and identifier
- distinct from message authentication



## User Authentication






## Means of User Authentication

- four means of authenticating user's identity
- based one something the individual
  - Knows
  - possesses
  - is (static biometrics)
  - does (dynamic biometrics)
  - Give examples of each
- can use alone or combined
- all can provide user authentication
- all have issues

## Password authentication

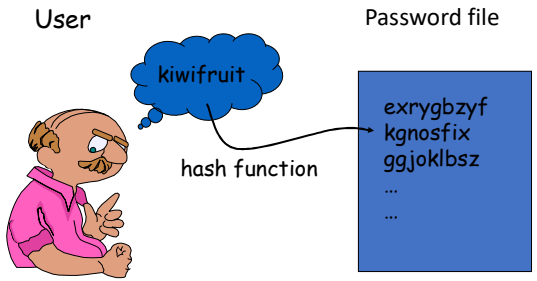
- Basic idea
  - User has a secret password
  - System checks password to authenticate user
- Issues
  - How is password stored?
  - How does system check password?
  - How easy is it to guess a password?
    - Difficult to keep password file secret, so best if it is hard to guess password even if you have the password file

## Password Authentication

- widely used user authentication method
  - user provides name/login and password
  - system compares password with that saved for specified login
- authenticates ID of user logging and
  - that the user is authorized to access system
  - determines the user's privileges
  - is used in discretionary access control



## Basic password scheme




## Basic password scheme

- Hash function h : strings → strings
  - Given h(password), hard to find password
  - No known algorithm better than trial and error
- User password stored as h(password)
- When user enters password
  - System computes h(password)
  - Compares with entry in password file
- No passwords stored on disk


# Use of Hashed Passwords

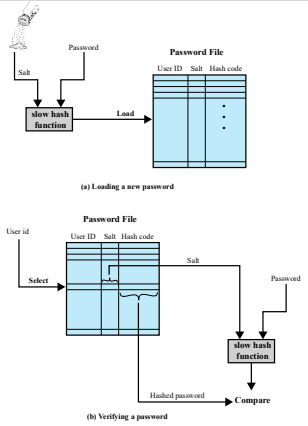



Figure 3.1 UNIX Password Scheme

## Improved Implementations

- have other, stronger, hash/salt variants
- many systems now use MD5
  - with 48-bit salt
  - password length is unlimited
  - is hashed with 1000 times inner loop
  - produces 128-bit hash
- OpenBSD uses Blowfish block cipher based hash algorithm called Bcrypt
  - uses 128-bit salt to create 192-bit hash value



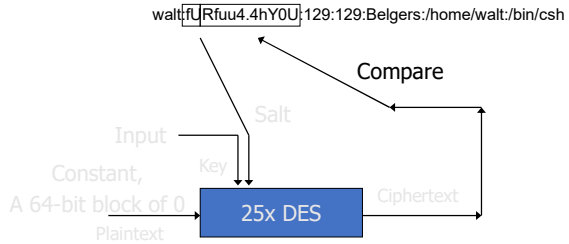
## UNIX Implementation

- original scheme
  - 8 character password form 56-bit key
  - 12-bit salt used to modify DES encryption into a one-way hash function
  - 0 value repeatedly encrypted 25 times
  - output translated to 11 character sequence
- now regarded as woefully insecure
  - e.g. supercomputer, 50 million tests, 80 min
- sometimes still used for compatibility



## Salt

- Password line



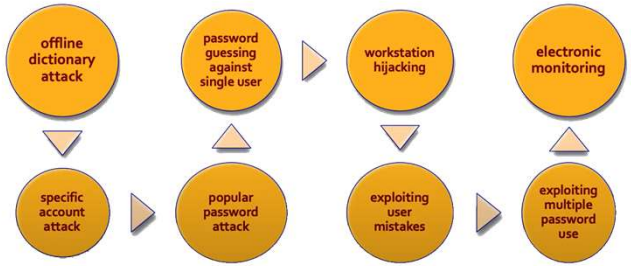

When password is set, salt is chosen randomly
12-bit salt slows dictionary attack by factor of $2^{12}$

## Password Cracking

- Dictionary attacks
  - try each word then obvious variants in large dictionary against hash in password file
- Rainbow table attacks
  - precompute tables of hash values for all salts
  - a mammoth table of hash values
  - e.g. 1.4GB table cracks 99.9% of alphanumeric Windows passwords in 13.8 secs
  - not feasible if larger salt values used
- Brute Force Attack



## Password Vulnerabilities






## Countermeasures

- stop unauthorized access to password file
- intrusion detection measures
- account lockout mechanisms
- policies against using common passwords but rather hard to guess passwords
- training & enforcement of password policies (L;m@$jj!)
- automatic workstation logout
- encrypted network links

## Password Choices

- users may pick short passwords
  - e.g. 3% were 3 chars or less, easily guessed
  - system can reject choices that are too short
- users may pick guessable passwords
  - so crackers use lists of likely passwords
  - e.g. one study of 14000 encrypted passwords guessed nearly 1/4 of them

## Password File Access Control

- can block offline guessing attacks by denying access to encrypted passwords
  - make available only to privileged users
  - often using a separate shadow password file
- still have vulnerabilities
  - exploit O/S bug
  - accident with permissions making it readable
  - users with same password on other systems
  - access from unprotected backup media
  - sniff passwords in unprotected network traffic



## Proactive Password Checking

- rule enforcement plus user advice, e.g.
  - 8+ chars, upper/lower/numeric/punctuation
  - may not suffice
- password cracker
  - time and space issues
- Markov Model
  - generates guessable passwords
  - hence reject any password it might generate
- Bloom Filter
  - use to build table based on dictionary using hashes
  - check desired password against this table



## Token Authentication

- object user possesses to authenticate, e.g.
  - embossed card
  - magnetic stripe card
  - memory card
  - smartcard



## Remote User Authentication

- authentication over network more complex
  - problems of eavesdropping, replay
- generally use challenge-response
  - user sends identity
  - host responds with random number
  - user computes f(r,h(P)) and sends back
  - host compares value from user with own computed value, if match user authenticated
- protects against a number of attacks

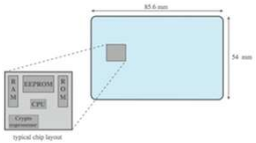
## Memory Card

- store but do not process data
- magnetic stripe card, e.g. bank card
- electronic memory card
- used alone for physical access
- with password/PIN for computer use
- drawbacks of memory cards include:
  - need special reader
  - loss of token issues
  - user dissatisfaction



## Smartcard

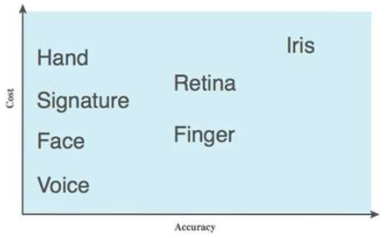
- credit-card like
- has own processor, memory, I/O ports
  - wired or wireless access by reader
  - may have crypto co-processor
  - ROM, EEPROM, RAM memory
- executes protocol to authenticate with reader/computer
- also have USB dongles





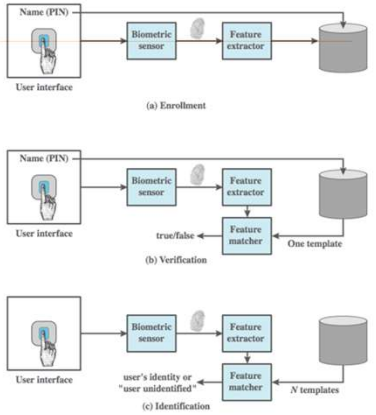

## Biometric Authentication

- authenticate user based on one of their physical characteristics



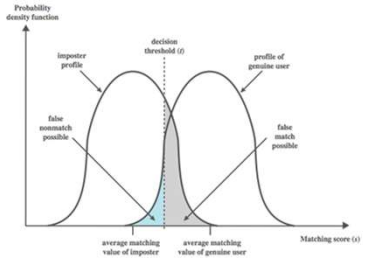



## Operation of a Biometric System



## Biometric Accuracy

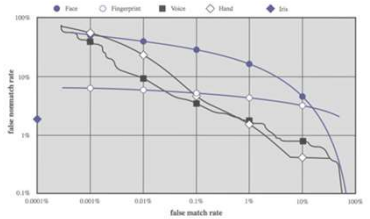
- never get identical templates
- problems of false match / false non-match






## Biometric Accuracy

- can plot characteristic curve
- pick threshold balancing error rates






## Authentication Security Issues

- client attacks
- host attacks
- eavesdropping
- replay
- trojan horse
- denial-of-service



## Summary

- introduced user authentication
  - using passwords
  - using tokens
  - using biometrics
- remote user authentication issues

## Means of User Authentication

- four means of authenticating user's identity
- based one something the individual
  - knows - e.g. password, PIN
  - possesses - e.g. key, token, smartcard
  - is (static biometrics) - e.g. fingerprint, retina
  - does (dynamic biometrics) - e.g. voice, sign
- can use alone or combined
- all can provide user authentication
- all have issues