KF School of Computing and Information Sciences
Florida International University

CNT 4403
Computing and Network Security

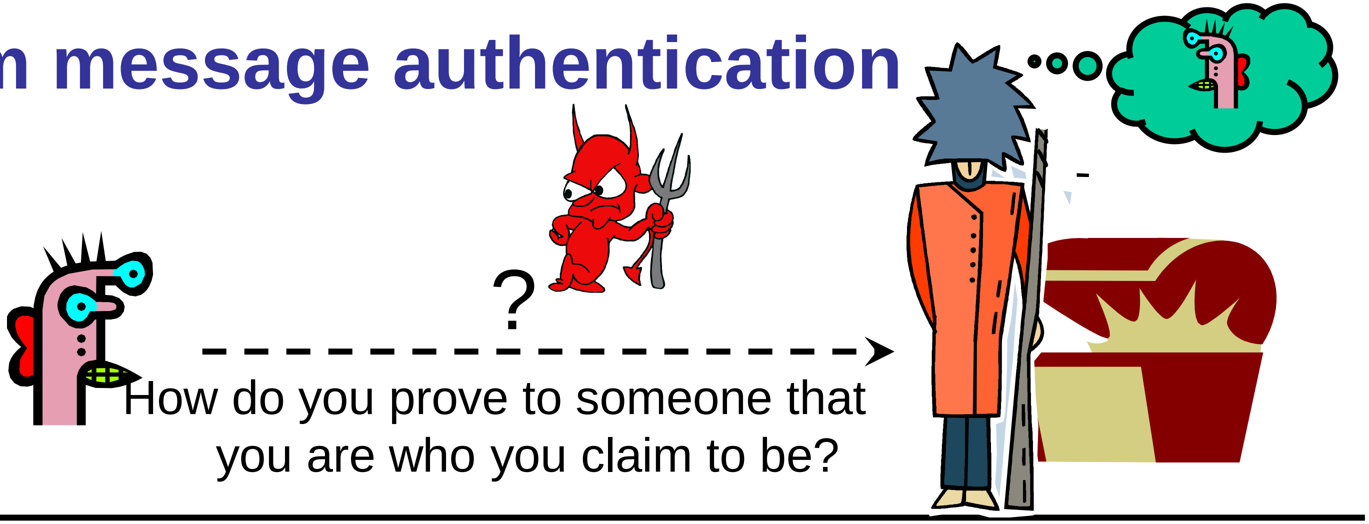
Access Control – User Authentication

Dr. Kemal Akkaya

E-mail: *kakkaya@fiu.edu*

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**



How do you prove to someone that you are who you claim to be?

Many Ways to Prove Who You Are

- **What you know**
  - Passwords
  - Secret key
- **Where you are**
  - IP address
- **What you are**
  - Biometrics
- **What you have**
  - Secure tokens
- **A combination of these can also be used**

Password-Based Authentication

- ❑ **Widely used user authentication method**
  - ➢ 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
- ❑ **How is the password communicated?**
  - ➢ Eavesdropping risk
- ❑ **How is the password stored?**
  - ➢ In the clear? Encrypted? Hashed?
- ❑ **How does the system check the password?**
- ❑ **How easy is it to guess the password?**
  - ➢ Easy-to-remember passwords tend to be easy to guess
  - ➢ Password file is difficult to keep secret

Other Aspects

- ❑ **Usability**
  - ➢ Hard-to-remember passwords?
  - ➢ Carry a physical object all the time?
- ❑ **Denial of service**
  - ➢ Stolen wallet
  - ➢ Attacker tries to authenticate as you, account locked after three failures
  - ➢ "Suspicious" credit card usage
- ❑ **Social engineering**

WHAT DOES MY FOREHEAD SAY?
scottadams@aol.com
www.dilbert.com
I KEEP FORGETTING MY PASSWORD, SO I WROTE IT ON MY HEAD.
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
IS YOUR PASS-WORD 123?
I JUST SAID I DON'T KNOW.

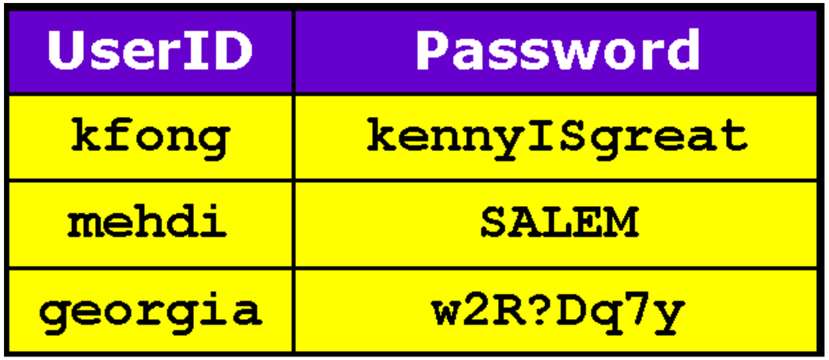
© Scott Adams, Inc./Dist. by UFS, Inc.

Passwords in the Real World

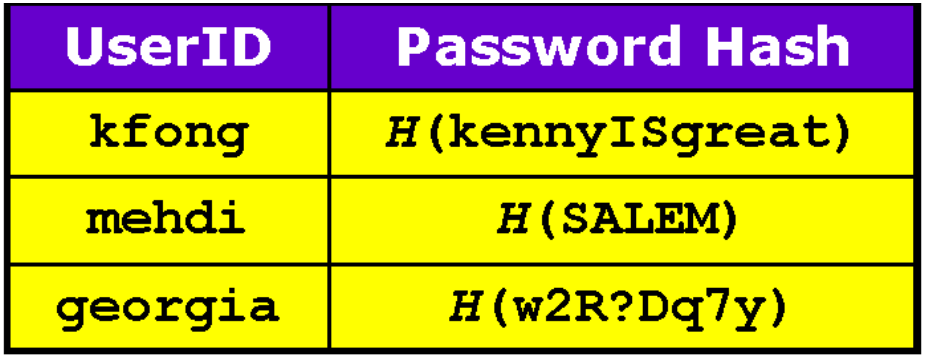
- ❑ **First step after any successful intrusion: install sniffer or keylogger to steal more passwords**
  - ➢ Second step: run cracking tools on password files
    - ✓ Usually on other hijacked computers
  - ➢ In Mitnick's "Art of Intrusion", 8 out of 9 exploits involve password stealing and/or cracking
- ❑ **Real-life Examples:**
  - ➢ From high school pranks…
    - ✓ Students in California change grades
      - – Different authentication for network login and grade system, but teachers were using the same password (very common)
  - ➢ …to serious cash
    - ✓ English accountant uses co-workers' password to steal $17 million for gambling
  - ➢ …to identity theft
    - ✓ Helpdesk employee uses passwords of a credit card database to sell credit reports to Nigerian scammers

Password Authentication

- ❑ **Basic Scheme**
  - ➢ Store user name and corresponding password in clear text
  - ➢ Problem: Anyone who has access to the password file can get the password.
- ❑ **Instead of user password, store H(password)**
- ❑ **When user enters password, compute its hash and compare with entry in password file**
  - ➢ System does not store actual passwords!
  - ➢ Difficult to go from hash to password!
    - ✓ Do you see why hashing is better than encryption here?



UserID	Password
kfong	kennyISgreat
mehdi	SALEM
georgia	w2R?Dq7y



UserID	Password Hash
kfong	*H*(kennyISgreat)
mehdi	*H*(SALEM)
georgia	*H*(w2R?Dq7y)

Password Authentication

❑ Dictionary Attack is possible with Hashing approach

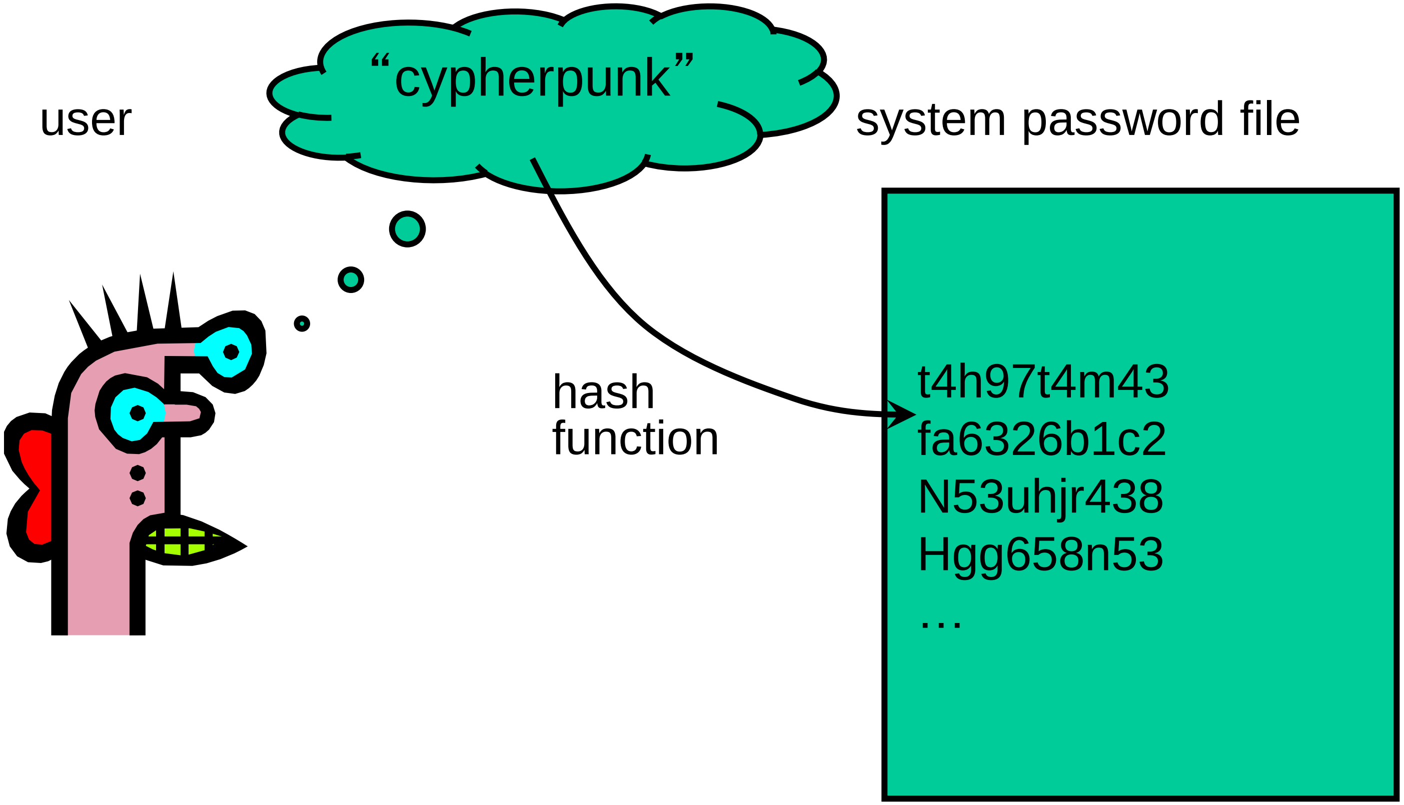
- ➢ i.e., Attacker can pre-compute H(word) for every word in the dictionary – this only needs to be done once!!
  - ✓ This is an offline attack
  - ✓ Once password file is obtained, cracking is instantaneous

❑ Salting is the solution for this problem

- ➢ The system generates a random string each time a password is reset
- ➢ The salt is stored in the file and concatenated with the password before hashed
  - ✓ With salt, attacker must compute hashes of all dictionary words once for each combination of salt value and password

UserID	Salt	Password Hash
kfong	DCFV	*H*(kennyISgreat,DCFV)
mehdi	PLRE	*H*(SALEM,PLRE)
georgia	ACCW	*H*(w2R?Dq7y,ACCW)

UNIX-Style Passwords



user

“cypherpunk”

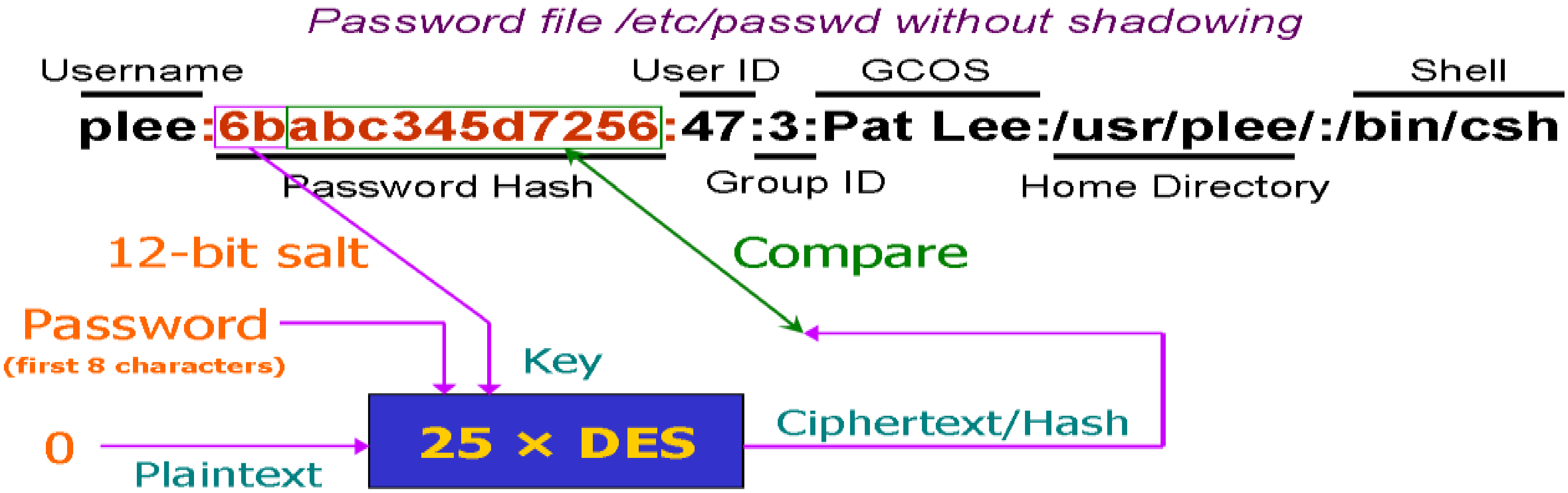
system password file

hash
function

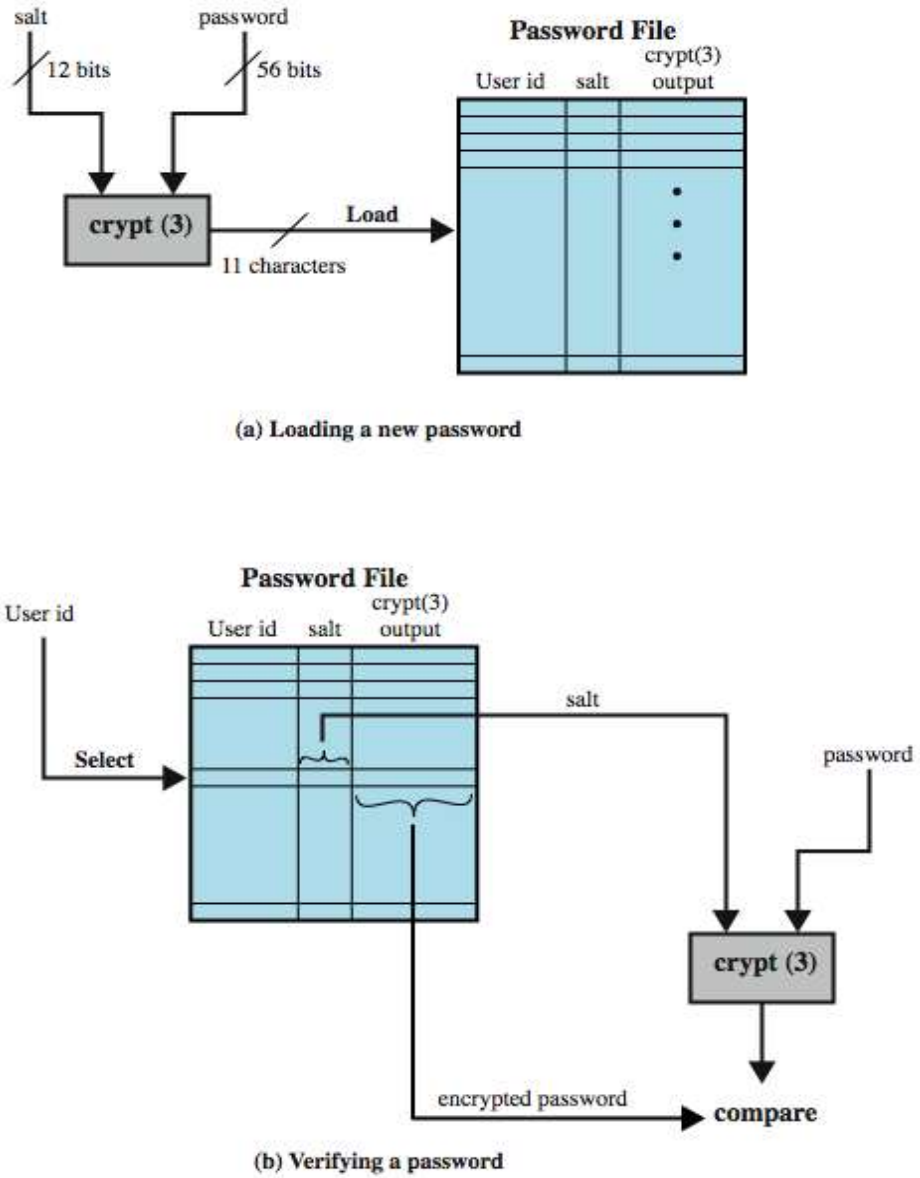
t4h97t4m43
fa6326b1c2
N53uhjr438
Hgg658n53
…

UNIX Passwords

- Uses a hash function called Crypt
  - Encrypt NULL string using password as the key
    - ✓ Truncates passwords to 8 characters!
  - Artificial slowdown: run DES 25 times
  - Can instruct modern UNIXes to use MD5 hash function or Blowfish



Password Checking



(a) Loading a new password

(b) Verifying a password

Password Security Risks

- Keystroke loggers
  - Hardware: KeyGhost, KeyShark, others
  - Software (spyware)
- Shoulder surfing
- Same password at multiple sites
- Broken implementations
- Social engineering
- Offline dictionary attack
- Popular password attack
- Password guessing against single user

Default Passwords

- **52 letters, 10 digits and 32 punctuation symbols: $94^8 \approx 6$ quadrillion possible 8-character passwords**
- **Examples from Mitnick's "Art of Intrusion"**
  - U.S. District Courthouse server: "public" / "public"
  - NY Times employee database: pwd = last 4 SSN digits
  - "Dixie bank": break into router (pwd="administrator"), then into IBM AS/400 server (pwd="administrator"), install keylogger to snarf other passwords
    - ✓ "99% of people there used 'password123' as their password"
- **U. of Michigan: 5% of passwords were "goblue"**
  - How many passwords on this campus involve "panthers", "gopanthers",etc.?

How People Use Passwords

- ❑ **Write them down**
- ❑ **Use a single password at multiple sites**
  - ➢ Do you use the same password for Amazon and your bank account? myFIU? Do you remember them all?
- ❑ **Make passwords easy to remember**
  - ➢ "password", "Kevin123", "popcorn"
- ❑ **Some services use "secret questions" to reset passwords**
  - ➢ "What is your favorite pet's name?"
  - ➢ Paris Hilton's T-Mobile cellphone hack

Social Engineering

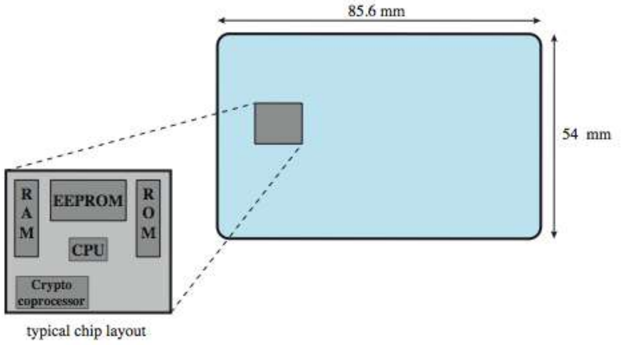
- ❑ **Univ. of Sydney study**
  - ➢ 336 CS students emailed asking for their passwords
    - ✓ Pretext: “validate” password database after suspected break-in
  - ➢ 138 returned their passwords; 30 returned invalid passwords; 200 reset passwords (not disjoint)
- ❑ **Treasury Dept. report (2005)**
  - ➢ Auditors pose as IT personnel attempting to correct a “network problem”
  - ➢ 35 of 100 IRS managers and employees provide their usernames and change passwords to a known value
- ❑ **Other examples: Mitnick’s “Art of Deception”**

Password Policies

- **A strong password should meet the following guidelines:**
  - Should be at least 8-characters long (now 16 characters)
  - Should have at least three of the following:
    - ✓ One or more uppercase letters (A-Z), one or more lowercase letter (a-z)
    - ✓ One or more digits (0-9), One or more special characters or punctuations marks (!@#$%^&*,.:;?)
  - Should not consist of dictionary words
  - Should never be the same as user name or contain the user name
  - Should not consist of user’s family member’s names, birth dates, pet names, etc.
  - Should be changed regularly (e.g., every 60-90 days)
- **Shared passwords should be forbidden**
- **Accounts and passwords should be reset as soon as they become invalid**
- **Limit the number of failed login attempts**
- **Never write down your password**

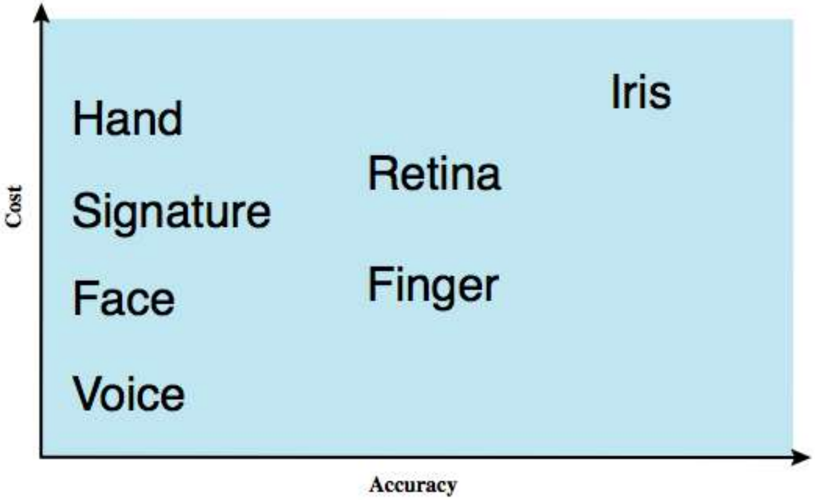
Alternative: Token Authentication

- **Object user possesses to authenticate, e.g.**
  - magnetic stripe card
  - memory card
    - ✓ store but do not process data
    - ✓ used alone for physical access
  - 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 response/challenge protocol to authenticate with reader/computer
  - Cryptographic calculators
  - Radio frequency identification (RFID) tags

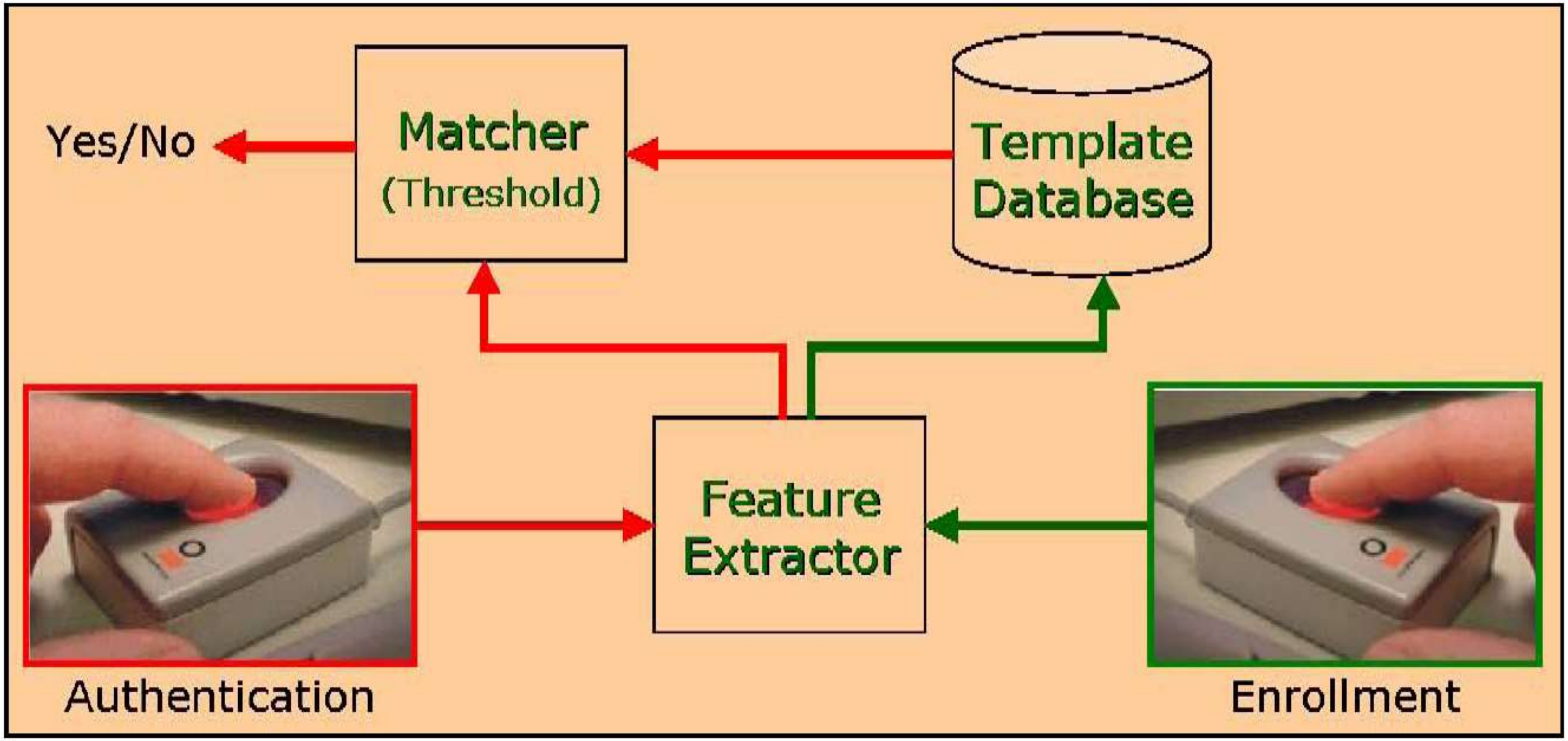


Biometric Authentication

- Authenticate user based on one of their physical characteristics
- Advantages
  - Never lost or forgotten
- Disadvantages
  - Cost
  - False positives/negatives
  - Privacy
  - Security and size of template DBs
  - Revocation after forgery

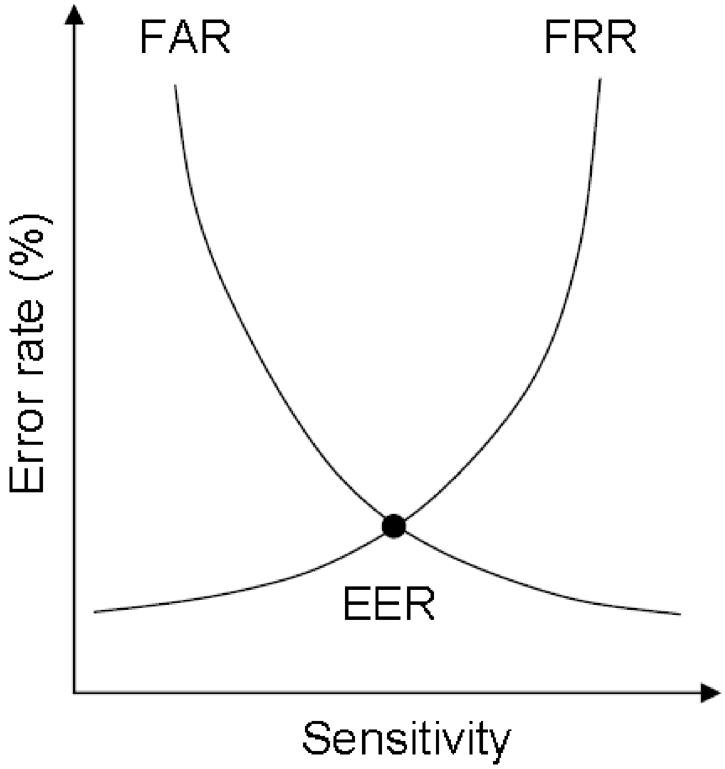


Operation of a Biometric System

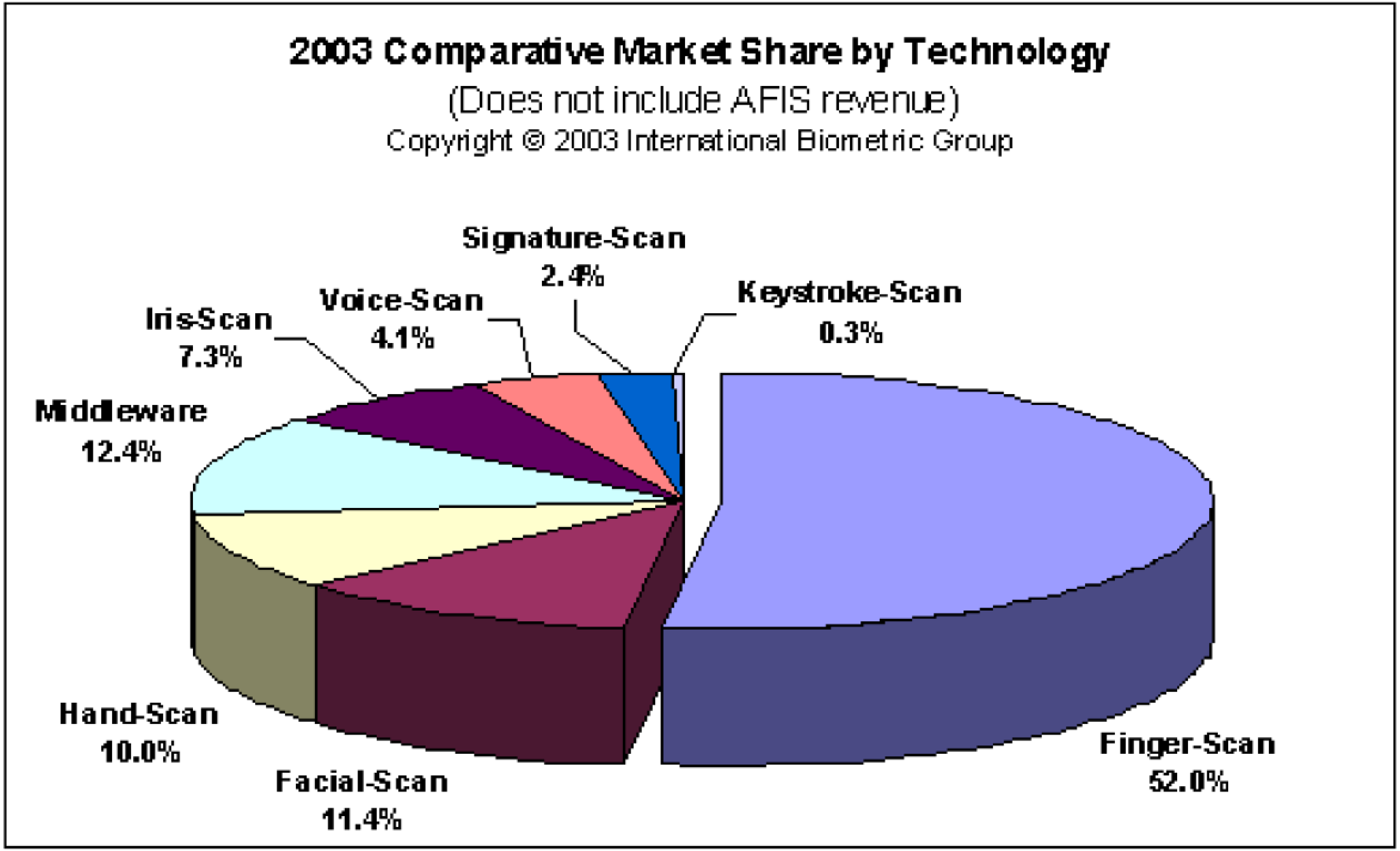


Biometric Accuracy

- ❑ **Never get identical templates**
- ❑ **Problems of false match / false non-match**
- ❑ **FAR: False Acceptance Rate**
- ❑ **FRR: False Rejection Rate**
- ❑ **EER: Equal Error Rate**
  - ➢ The threshold of the system set to the point at which EER occurs

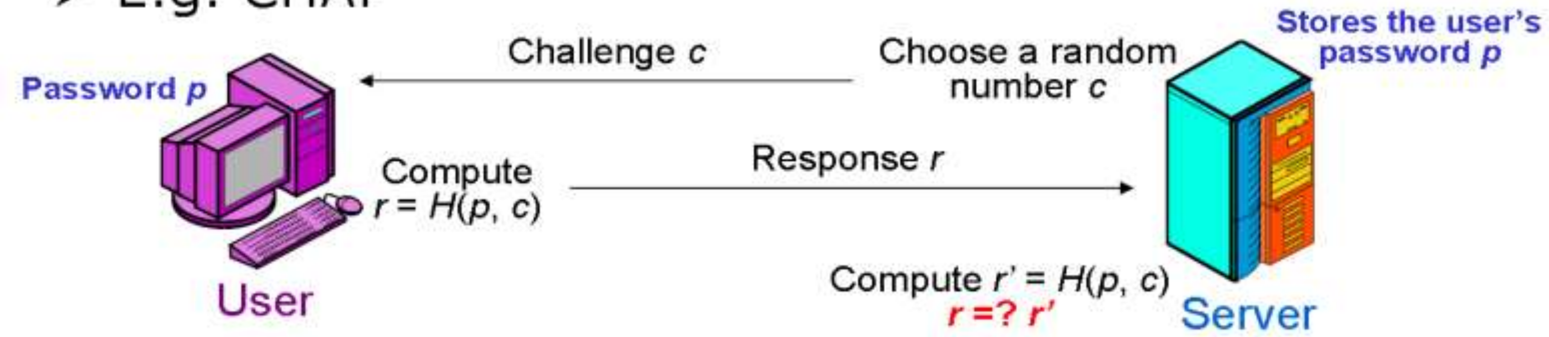


Biometric Technologies



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**
  - ➢ Passwords are not sent over network (i.e., no eavesdropping)
  - ➢ E.g. CHAP

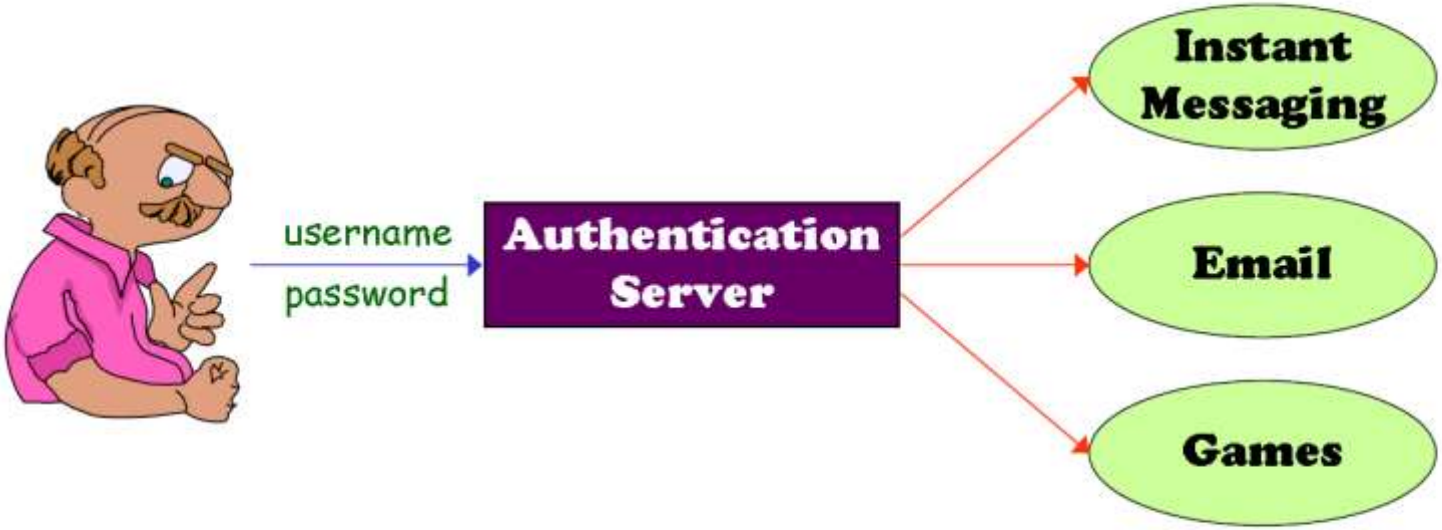


Multi-factor Authentication

- Adding a second factor for authentication
- This is in addition to the main mechanism (password etc).
- Can be through text message, phone call, biometrics, cards, etc.
  - What is my FIU’s multi-factor mechanism?
- If the password is compromised, second level authentication will fail.
- Became pretty common now
  - Usability is an important challenge here
    - ✓ Would you use a smart watch which can authenticate your type pattern?

Single Sign-On

- **A mechanism that enables a user to authenticate once with a single password and gain access to resources from multiple systems**
- **Eliminates the need for memorizing multiple passwords**
- **E.g., Windows Live ID**
  - Largest single sign-on service on the Web
  - Used by Hotmail, Xbox Live, Expedia, etc.


username
password
Authentication Server
Instant Messaging
Email
Games