

# **Authentication and Access Control**

---

**CS-576 Systems Security**

Instructor: Georgios Portokalidis

Fall 2018

# Overview

---

## Authentication vs Authorization

### Different means of authentication

- Attacks and good practices

### Different types of authorization

# Authentication vs Authorization

---

**Authentication** is the process of verifying an identity claimed by or for a system entity.

**Authorization** is the function of specifying access rights to resources related to information security and computer security in general and to **access control** in particular.

# Means/Factors of Authentication

Something the individual knows

Something the individual possesses

Something the individual is/does

# Something the User Knows

## Password

As56kf#dfjd8%d

John123

JustinBieber14

Y3llow5ubm4rine

## PIN

123456

654321

1248

338

## Answers (to questions)

What is the name of your dog?

What is your favorite color?

What... is the air-speed velocity of an unladen swallow?



← Friday Squid Blogging: How to Capture a Giant Squid

## Secret Questions

In 2004, I wrote about the prevalence of secret questions as backup passwords. The problem is that the answers to these "secret questions" are often much easier to guess than random passwords. Mother's maiden name isn't very secret. Name of first pet, name of favorite teacher: there are some common names. Favorite color: I could probably guess that in no more than five attempts.

Participants forgot **20%** of their own answers within six months.

Here's some actual research on the issue:

It's no secret: Measuring the security and reliability of authentication via 'secret' questions

Abstract:

All four of the most popular webmail providers -- AOL, Google, Microsoft, and Yahoo! -- rely on personal questions as the secondary authentication secrets used to reset account passwords.

all of which p  
of the questi  
these questi  
Acquaintanc

passwords were able to guess 17% of their answers. Participants forgot 20% of their own answers within six months. What's more, 13% of answers could be guessed within five attempts by guessing the most popular answers of other participants, though this weakness is partially attributable to the geographic homogeneity of our participant pool.

Tags: [academic papers](#), [authentication](#), [Microsoft](#), [passwords](#), [security questions](#)

Posted on May 25, 2009 at 9:56 AM • 80 Comments

Like Tweet +1

blog essays whole site

Subscribe



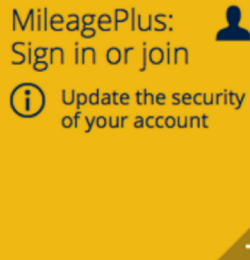
articles, and academic papers. Currently, I'm the Chief Technology Officer of Co3 Systems, a fellow at Harvard's Berkman Center, and a board member of EFF.

Related Entries

Breaking Microsoft's PPTP Protocol

It's no secret: Measuring the security and reliability of authentication via 'secret' questions

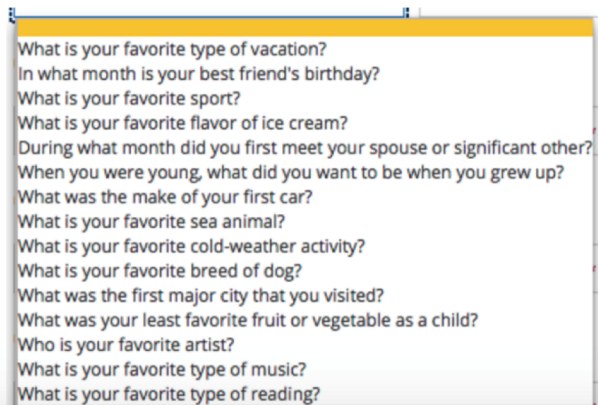
<http://research.microsoft.com/apps/pubs/default.aspx?id=79594>



## United Mileage Plus

Yesterday, Yan Zhu (@bcrypt) pointed out on Twitter that United Airlines Mileage Plus program has started collecting answers to security questions. They have a new twist: you must select one of a menu of answers.

United wants the answers to five questions, chosen from a list:



# Something the User Possesses



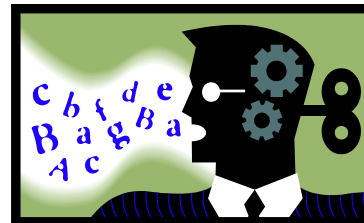
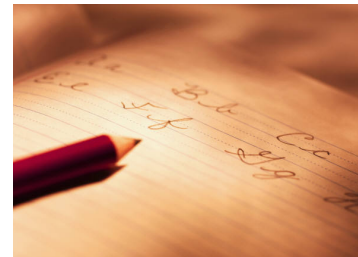


# Something the Individual...

..Is



..does



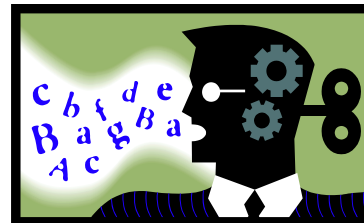
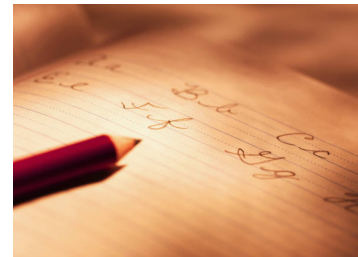
# Something the Individual...

..Is

..does



NOT just face  
recognition

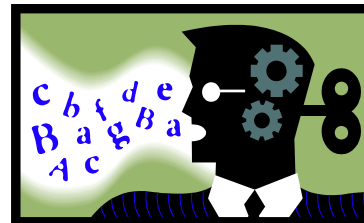
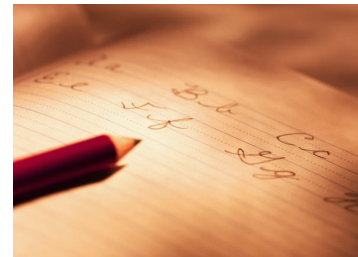


# Something the Individual...

..Is

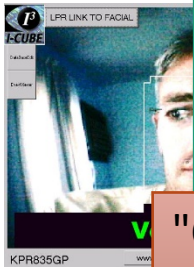


..does



# Something the Individual...

..Is



## How about CAPTCHA?

A screenshot of the reCAPTCHA website interface. The page features the reCAPTCHA logo on the left, a navigation menu with links like 'HOME', 'WHAT IS reCAPTCHA', 'WHAT IS A CAPTCHA SECURITY', 'GET reCAPTCHA', 'MY ACCOUNT', 'EMAIL PROTECTION', and 'RESOURCES'. The main content area displays a CAPTCHA challenge with the words 'and' and 'Luckyknow' in a distorted font. Below the challenge is a text input field with the prompt 'Type the two words:', a 'Submit' button, and a small reCAPTCHA logo with the tagline 'stop spam. read books.'. A footer note states: 'The words above come from scanned books. By typing them, you help to digitize old texts.'

"Completely Automated Public Turing test to tell Computers and Humans Apart"

# Multi-factor Authentication (MFA)

Require more than one methods/factors of authentication to be used

- Not of the same type! For example, two passwords.

Most common instantiation: two-factor authentication (2FA)

# Passwords

---

Widely used

Process

- User provides name/login and password
- System compares password with the one stored for that specified login

The user ID:

- Determines that the user is authorized to access the system
- Determines the user's privileges
- Is used in discretionary access control

# Password Transmission

HTTP



username: bob  
password: p4ssw0rd

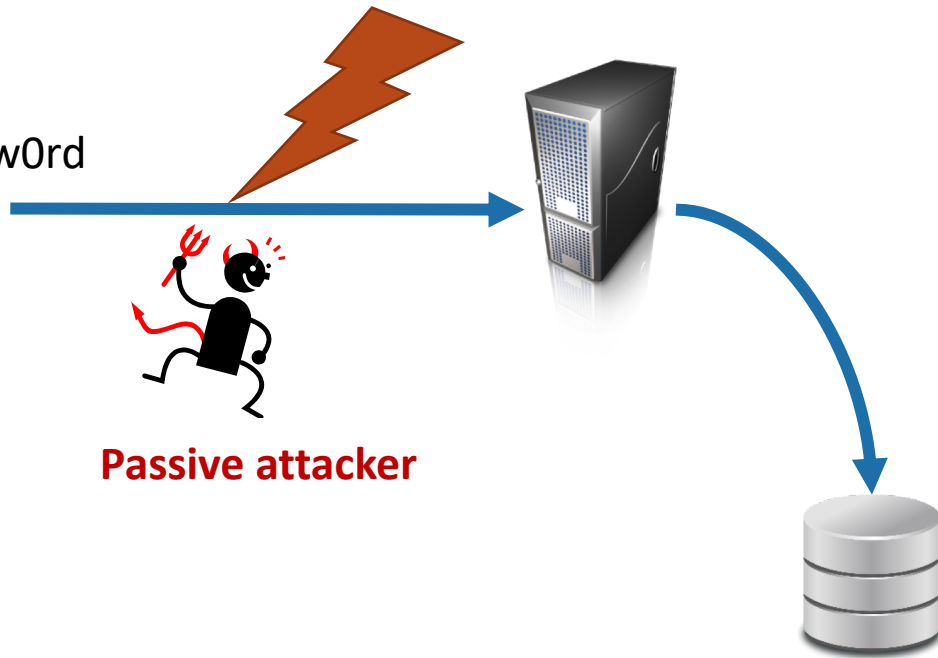


# Password Transmission

HTTP



username: bob  
password: p4ssw0rd





# Password Transmission

HTTP

HTTPS (TLS)



username: bob

password: p4ssw0rd



# Password Transmission

HTTP

HTTPS (TLS)



username: bob  
password: p4ssw0rd



**Passive attacker**



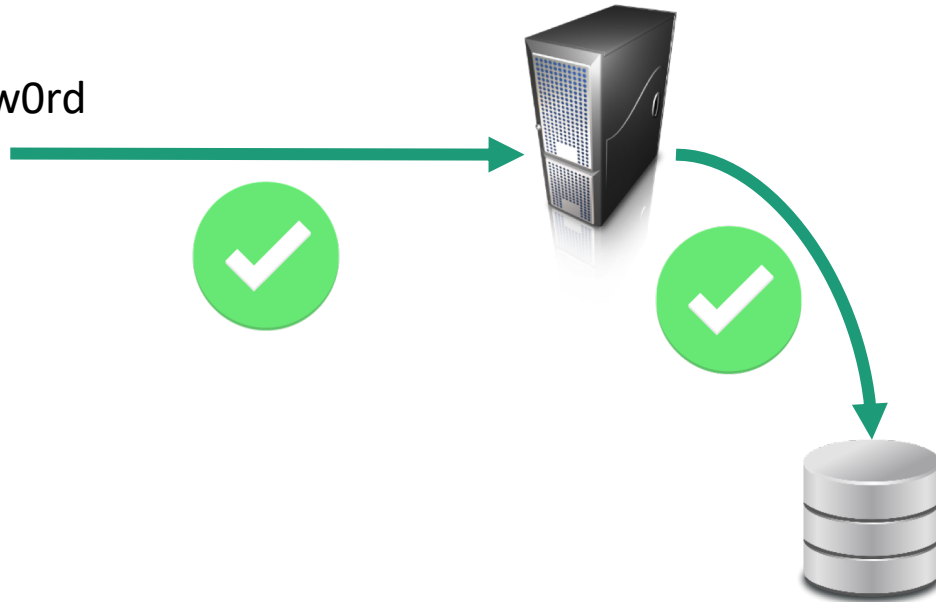
# Password Transmission

HTTP

HTTPS (TLS)



username: bob  
password: p4ssw0rd



End-to-end  
security  
necessary

# Password Storage

HTTP

HTTPS (TLS)



username: bob  
password: p4ssw0rd



**Raw**

username: bob

password: p4ssw0rd

# Password Storage

HTTP

HTTPS (TLS)



username: bob  
password: p4ssw0rd



**Password DB leak**



**Raw**

username: bob

password: p4ssw0rd



# Password Storage

HTTP

HTTPS (TLS)



username: bob  
password: p4ssw0rd



Insider



Password DB leak



Raw

username: bob
password: p4ssw0rd



# Password Leaks Happen All the Time

2009	RockYou Gaming	32.0 million
2010	Gawker Media <i>Domino attack prompted resets in other sites</i>	1.5 million
2011	Sony	1.0 million
2012	LinkedIn	6.5 million
2013	Twitter <i>Before being detected and shut down</i>	250,000
2013	Adobe	150.0 million
2015	ashley madison	<b>15.26 million</b>





# Security of Hash Functions

There are two approaches to attacking a secure hash function:

- **Cryptanalysis:** Exploit logical weaknesses in the algorithm
- **Brute-force attack:** Strength of hash function depends solely on the length of the hash code produced by the algorithm

MD5 and SHA-1 have been broken through cryptanalysis  
SHA-2 or later is suggested

# Password Cracking

---

Dictionary attacks

Brute-force

Combination of the above

**John the Ripper** – first open-source password cracker developed in 1996

# Dictionary Attacks

Develop a large dictionary of possible passwords and try each against the password file

Each password must be hashed and then compared to stored hash values

Good dictionaries and heuristics for combining words give attackers an advantage

Publicly available databases of cracked passwords also help

# Dictionary Attacks

Develop a large dictionary of possible passwords and try each against the password file

Each password must be hashed and then compared to stored hash values

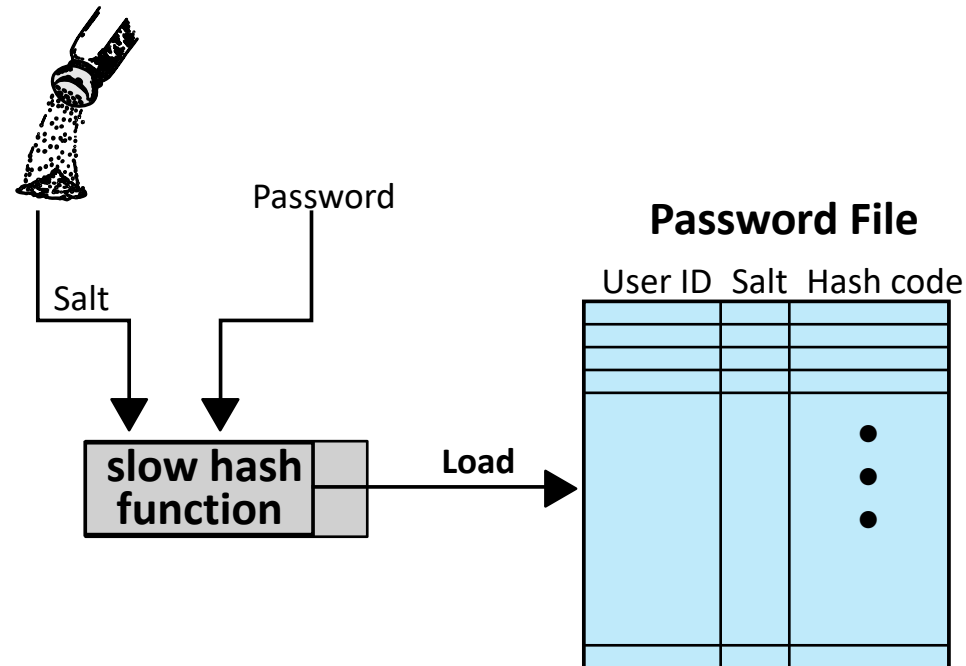
## Rainbow Table Attacks

- Pre-compute tables of hash values
- Greatly accelerate attacking hashes



# Adding Salt

A unique (possibly random) value (the salt) is added to the password before hashing



# Adding Salt

A unique (possibly random) value (the salt) is added to the password before hashing

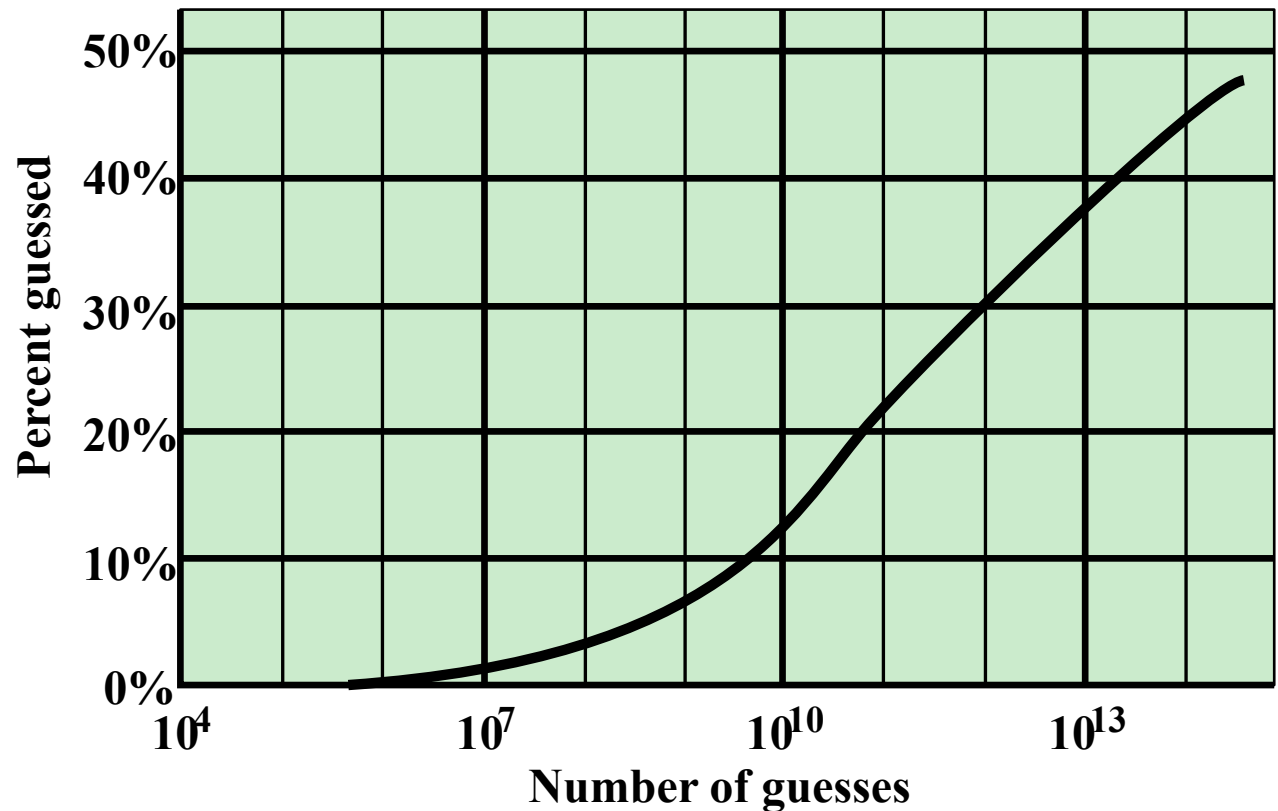


## Salts

- Make prevent the use of rainbow tables
- Make password attacks more expensive
- Hide whether multiple users use the same password

# Efficiency of Password Attacks

Using DB of leaked password files, including the RockYou file.





# CloudCracker

An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.

**Start Cracking** ?

File Type:

Handshake File:  No file selected.

SSID (Network Name):

Handshake   Dictionary   Delivery

**Big. Fast. Cheap.**  
 Run your network  
 handshake against  
**300,000,000 words**  
**in 20 minutes**  
**for \$17.**

"Welcome to the future: cloud-based WPA cracking is here!"  
 -- TechRepublic

"Low cost service cracks wireless passwords from the cloud..."  
 -- TheRegister

"This really is a great idea." -- Hacker News

### Save Money. Save Time.



Whether it's a WPA2 network, NTLM hashes, Unix hashes, or an encrypted PDF file, one thing's for certain. By specializing in optimized cracking solutions and by fine-tuning dictionaries from iteration to iteration, we can provide a solution that's more effective, faster, and cheaper than anything else.

### Comprehensive Dictionaries.



We have a range of dictionaries, fine-tuned for the format at hand. By extrapolating from our successes and iterating over our failures, we've been able to converge on the most effective wordlists for the money, every time.

### Feel Safe Knowing We Found It. Feel Secure If We Don't.



Our jobs cost the same whether we find

### Simple To Use.



Submit your job in three quick steps,

<https://www.cloudcracker.com/>



An online password cracking service for penetration testers and network auditors who need to check the security of wireless networks, crack password hashes and perform password encryption.

### Start Cracking


File Type:

Handshake File:

SSID (Network Name):

[Handshake](#) [Dictionary](#) [Delivery](#)

**Save Money. Save Time.**




Whether it's a WPA2 network, NTLM hashes, Unix hashes, or an encrypted PDF file, one thing's for certain. By specializing in optimized cracking solutions and by fine-tuning dictionaries from iteration to iteration, we can provide a solution that's more effective, faster, and cheaper than anything else.

**Comp**

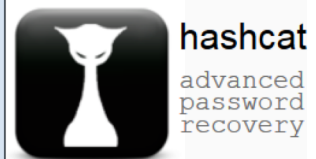
We have fine-tuned extrapolating and iterating algorithms able to crack wordlists

**Feel Safe**

**Feel Secure If We Don't.**



Our jobs cost the same whether we find



- hashcat
- 
- oclGaussCrack
- Forum
- Wiki
- Trac
- Tools
- Events
- Converter
- Contact

### Download latest version

Name	Version	md5sum
oclHashcat for AMD	<a href="#">v1.30</a>	4e6e77bbdb15df534348f7745dbc5d0a
oclHashcat for NVidia	<a href="#">v1.30</a>	1e17da4d927c6745c560af2c608337aa

### GPU Driver requirements:

- NV users require ForceWare 331.67 or later
- AMD users require Catalyst 14.6b or later

### Features

- **Worlds fastest password cracker**
- **Worlds first and only GPGPU based rule engine**
- Free
- Multi-GPU (up to 128 gpus)
- Multi-Hash (up to 100 million hashes)
- Multi-OS (Linux & Windows native binaries)
- Multi-Platform (OpenCL & CUDA support)
- Multi-Algo (see below)
- Low resource utilization, you can still watch movies or play games while cracking
- Focuses highly iterated modern hashes
- Focuses dictionary based attacks
- Supports distributed cracking
- Supports **pause / resume** while cracking
- Supports sessions
- Supports restore
- Supports reading words from file
- Supports reading words from **stdin**
- Supports hex-salt
- Supports hex-charset
- Built-in benchmarking system
- Integrated **thermal watchdog**
- [100+ Algorithms](#) implemented with performance in mind
- ... and much more

### hashcat Screenshot

```

root@sf:~/oclHashcat-1.30# ./oclHashcat64.bin -m 23 -a 3 -t 60 hash
oclHashcat v1.30 starting...

Device #1: Hawaii, 3072MB, 1000Mhz, 44MCU

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes
Applicable Optimizers:
+ Zero-Byte
    
```

<http://hashcat.net/oclhashcat/>

# RISK ASSESSMENT / SECURITY & HACKTIVISM

## 25-GPU cluster cracks every standard Windows password in <6 hours

All your passwords are belong to us.

by Dan Goodin - Dec 10, 2012 12:00 am UTC

Share Tweet 266



Welcome to Radeon City, population: 8. It's one of five servers that make up a high-performance password-cracking cluster.

Jeremi Gosney

A password-cracking expert has unveiled a computer cluster that can cycle through as many as 350 billion guesses per second. It's an almost unprecedented speed that can try every possible Windows passcode in the typical enterprise in less than six hours.

### LATEST FEATURE STORY

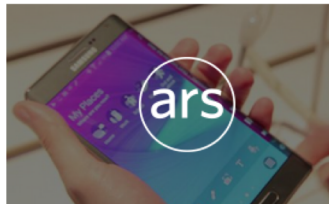


FEATURE STORY (3 PAGES)

#### Review: In its second generation, the Moto X becomes a true flagship

We miss the smaller size, but everything about this \$499 phone feels high-end.

### WATCH ARS VIDEO



#### Samsung Unpacked 2014

We take on Samsung's truckload of new devices.

### STAY IN THE KNOW WITH



### LATEST NEWS

rule engine

views or play games while cracking

in mind

```
clHashcat64.bin -m 23 -a 3 -t 60 hash
```

```
0MHz, 44MCU
```

```
ests, 1 unique salts  
0x000000ff mask, 1024 bytes
```

# Bcrypt()

**bcrypt** is a password hashing function designed by Niels Provos and David Mazières, based on the Blowfish cipher

**bcrypt** is an adaptive function:

- over time, the iteration count can be increased to make it slower
- It can remain resistant to brute-force search attacks

# Password Reuse

---

Users tend to reuse the same password with multiple accounts

- Exposure of one password leads to compromise of multiple passwords
- Strong measures adopted by security-aware services can be invalidated by careless services

# Phishing

www.sanagustinturismo.co/Facebook/

facebook

Email

Stay logged in

Password

Enter

[Forgot your password?](#)



## Connect with your friends faster, wherever you are.

The Facebook application is available in more than 2,500 phones.

- Faster navigation
- Compatible with the camera and your phone contacts
- Without regular updates: download only

[Discover Facebook Mobile](#)

## Sign up

It's free (and will remain).

Name:

Surname:

Your email:

Re-enter your email address:

Password:

Gender:

Select sex:

Date of Birth:

Day:

Month:

Year:

Why do I have to provide my birthday?

[Sign up](#)

# Phishing

Bank of America | Home | P x

Bank of America Corporation [US] https://www.bankofamerica.com feross.org is now full screen. Exit full screen (Esc)

Personal Small Business Wealth Management Businesses & Institutions About Us

Locations Contact us Help En español Search Bank of America

Bank Borrow Invest Protect Plan

Enter Your Online ID Sign In Enroll

Save this Online ID

Select account location

Help/options

Bank of America

Online Banking

Take charge of your money with 24/7 access

Get started

Know your balance

Stay up to date

Get alerts

Fake  
Browser  
with URL  
using  
HTML 5

# Password Managers

A password manager offers an encrypted “wallet” for storing username/password pairs

Protected by password-based encryption

- A master password is used to derive a key for decrypting (unsealing) the wallet

Can defeat phishing, password reuse, poor password choices by

- Automatically filling in password based on domain
- Automatically generating strong passwords
- Eliminating the need to remember many passwords

# Password Managers

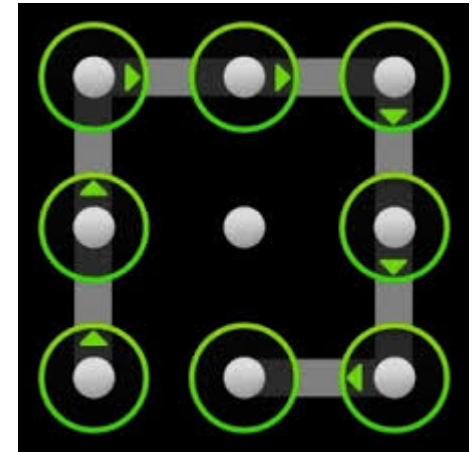
---

## Weaknesses:

- Compromise of the master password/wallet can be catastrophic
- Software may suffer from vulnerabilities



# Alternatives -- Graphical Passwords

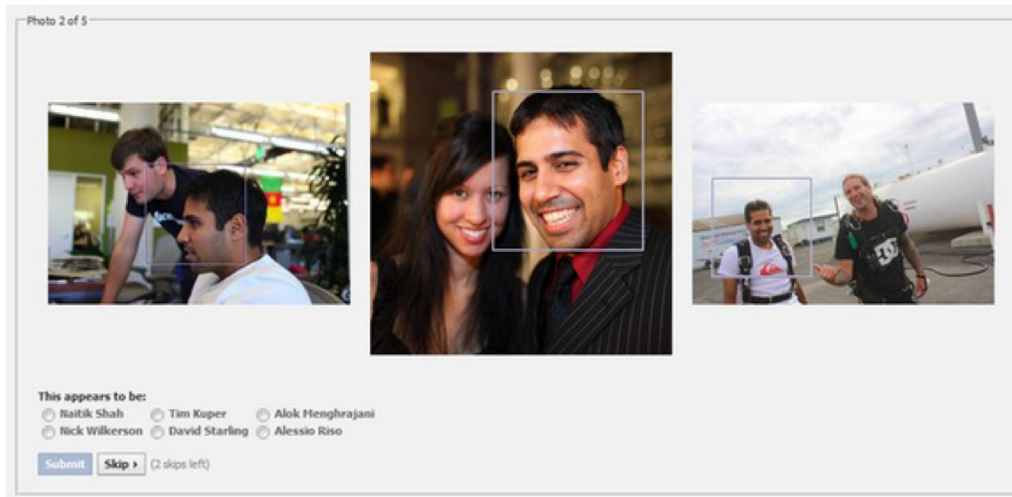


# Alternatives -- Social Authentication



Traditional captcha

Instead of showing you a traditional captcha on Facebook, one of the ways we may help verify your identity is through social authentication. We will show you a few pictures of your friends and ask you to name the person in those photos. Hackers halfway across the world might know your password, but they don't know who your friends are.



# Token-based Authentication

---

## Two major types

- Memory based (dumb) tokens
- Smart tokens

# Memory Cards

Can store but do not process data

The most common is the magnetic stripe card

Can include an internal electronic memory

Can be used alone for physical access

- Hotel room
- ATM

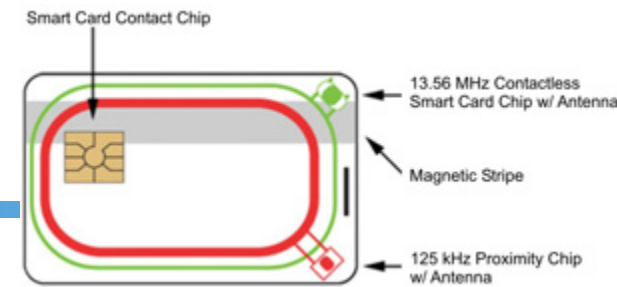
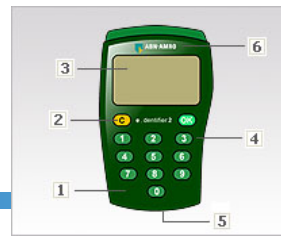
Provides significantly greater security when combined with a password or PIN

Drawbacks of memory cards include:

- Requires a special reader
- Can be stolen
- User needs to carry them



# Smart Tokens



## Physical characteristics:

- Include an embedded microprocessor
- A smart token that looks like a bank card
- Can look like calculators, keys, small portable o

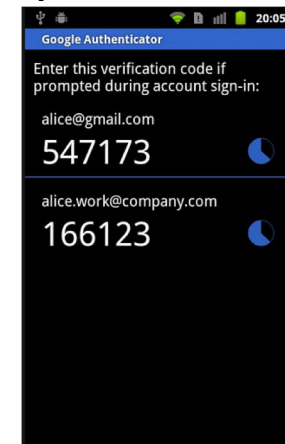


## Interface:

- Manual interfaces include a keypad and display for interaction
- Electronic interfaces communicate with a compatible reader/writer

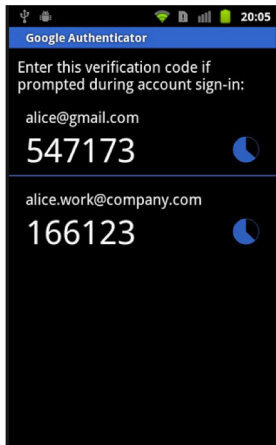
## Authentication protocol:

- Two main categories:
  - Dynamic password generator
  - Challenge-response



# Dynamic Protocol

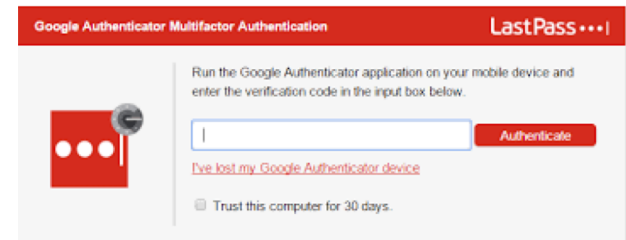
## Time-based One Time Password Generation



SECRET

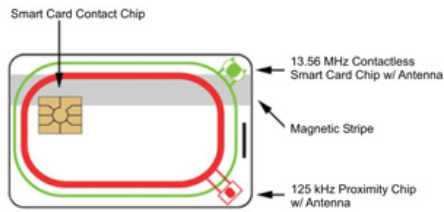
Valid for a limited amount of time

OTP

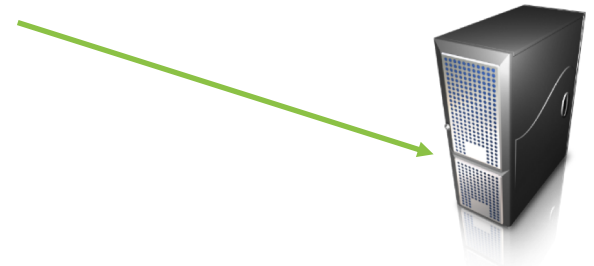


SECRET

# Simple Mutual Authentication (Challenge-Response)



$\text{secret} = H(\text{password})$



Server sends  $sc$



Generate unique random value  $sc$   
(nonce)

Generate unique random value  $cc$   
and calculate  
 $cr = H(cc + sc + \text{secret})$

Client sends  $cr + cc$



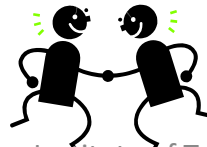
Generate  $cr$  and check received  
value

Generate  $sr$  and check  
received value

Server sends  $sr$



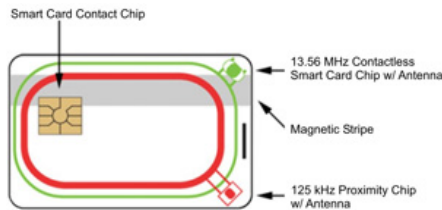
Generate  
 $sr = H(sc + cc + \text{secret})$



# Challenge-Response Protocol

Using public-key cryptography

Secret key  $PK^+$



Public key  $PK^-$



Verify signature

Generate unique random value  $cc$

Server sends  $sc + \text{SIG}(PK^-, sc)$

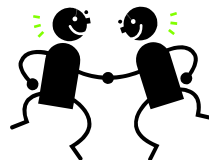


Generate unique random value  $sc$  (nonce)

Client sends  $cr + \text{SIG}(PK^+, cr)$



Verify signature





# Security Issues with Cards

Information may be unencrypted on the card

They can be reverse engineered



# Biometric Authentication

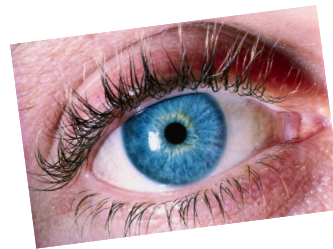
Attempts to authenticate an individual based on unique physical characteristics

Based on pattern recognition

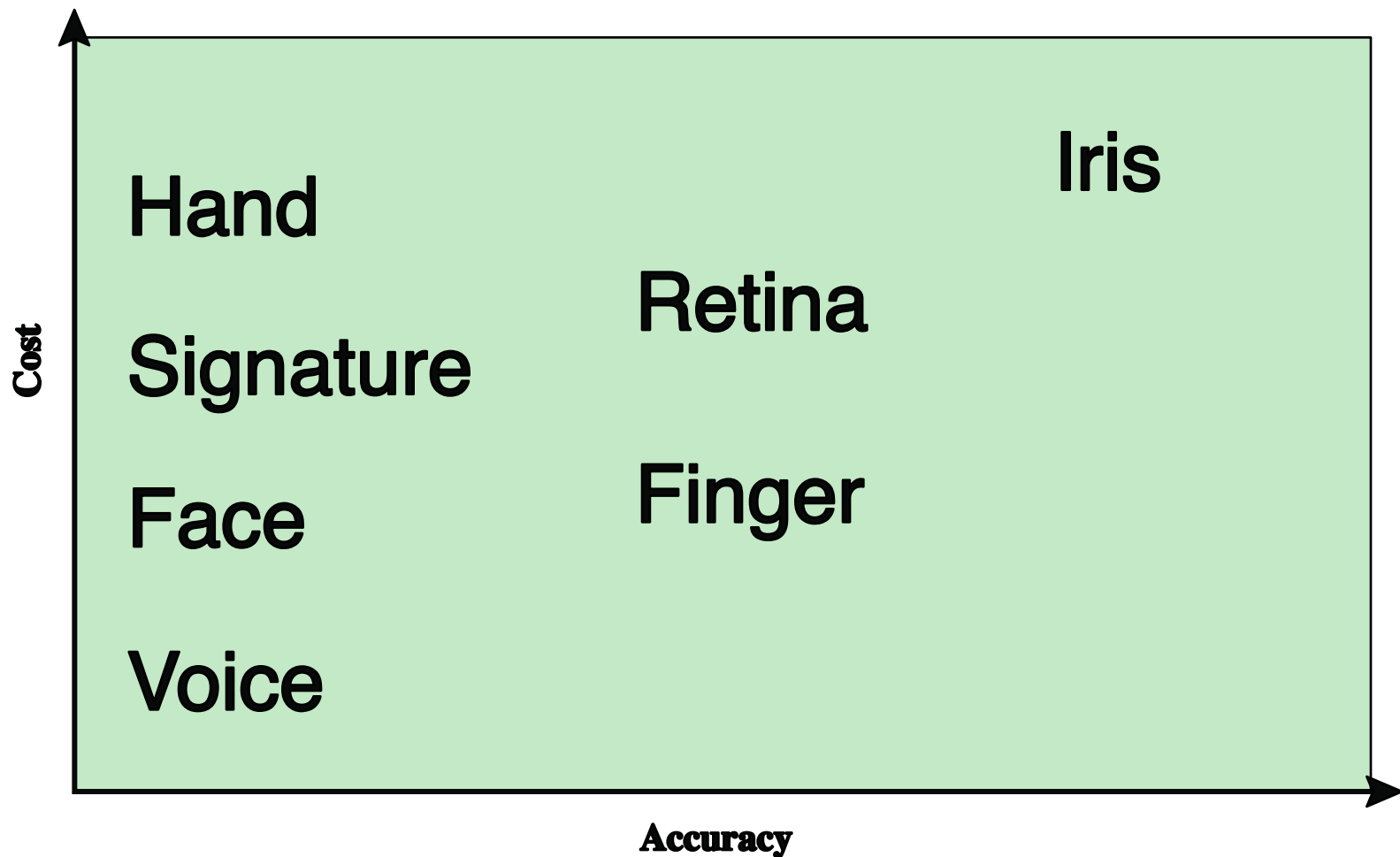
Is technically complex and expensive when compared to passwords and tokens

Physical characteristics used include:

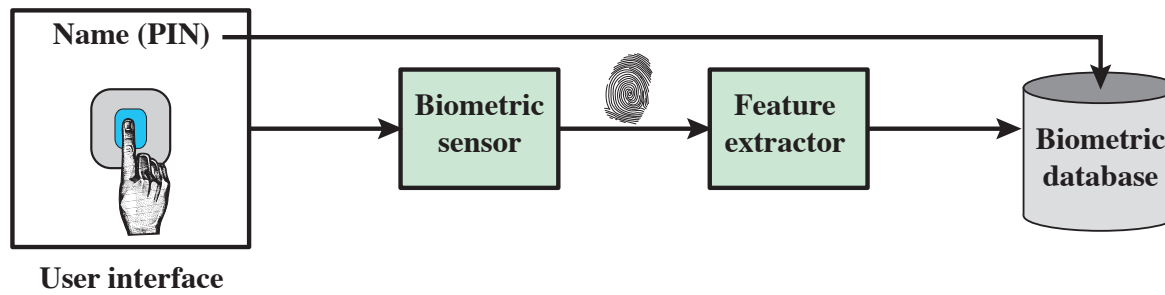
- Facial characteristics
- Fingerprints
- Hand geometry
- Retinal pattern
- Iris
- Signature
- Voice



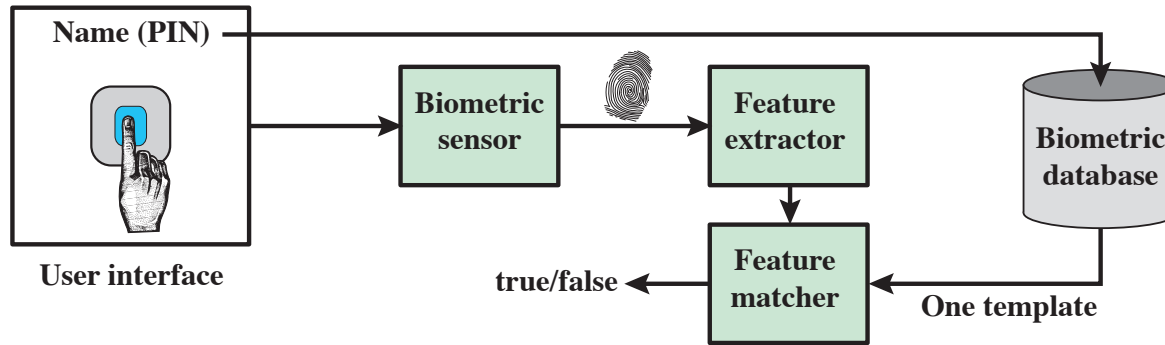
# Cost vs Accuracy for Biometrics



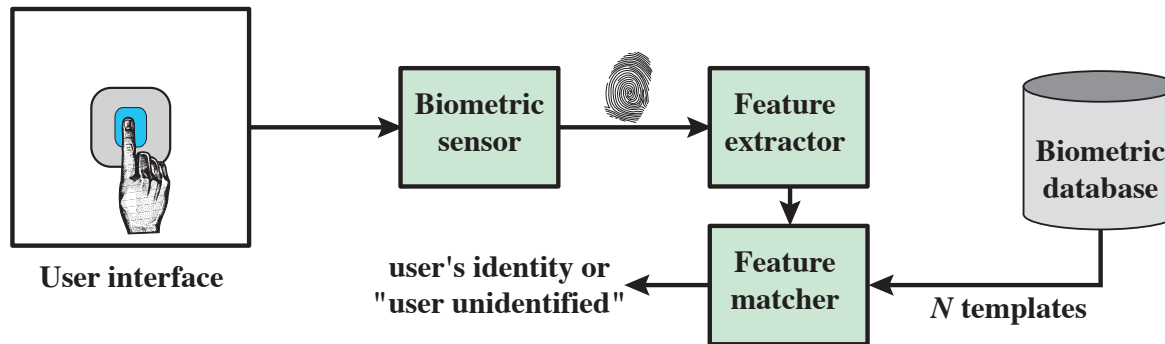
# Using Physical Biometrics



(a) Enrollment

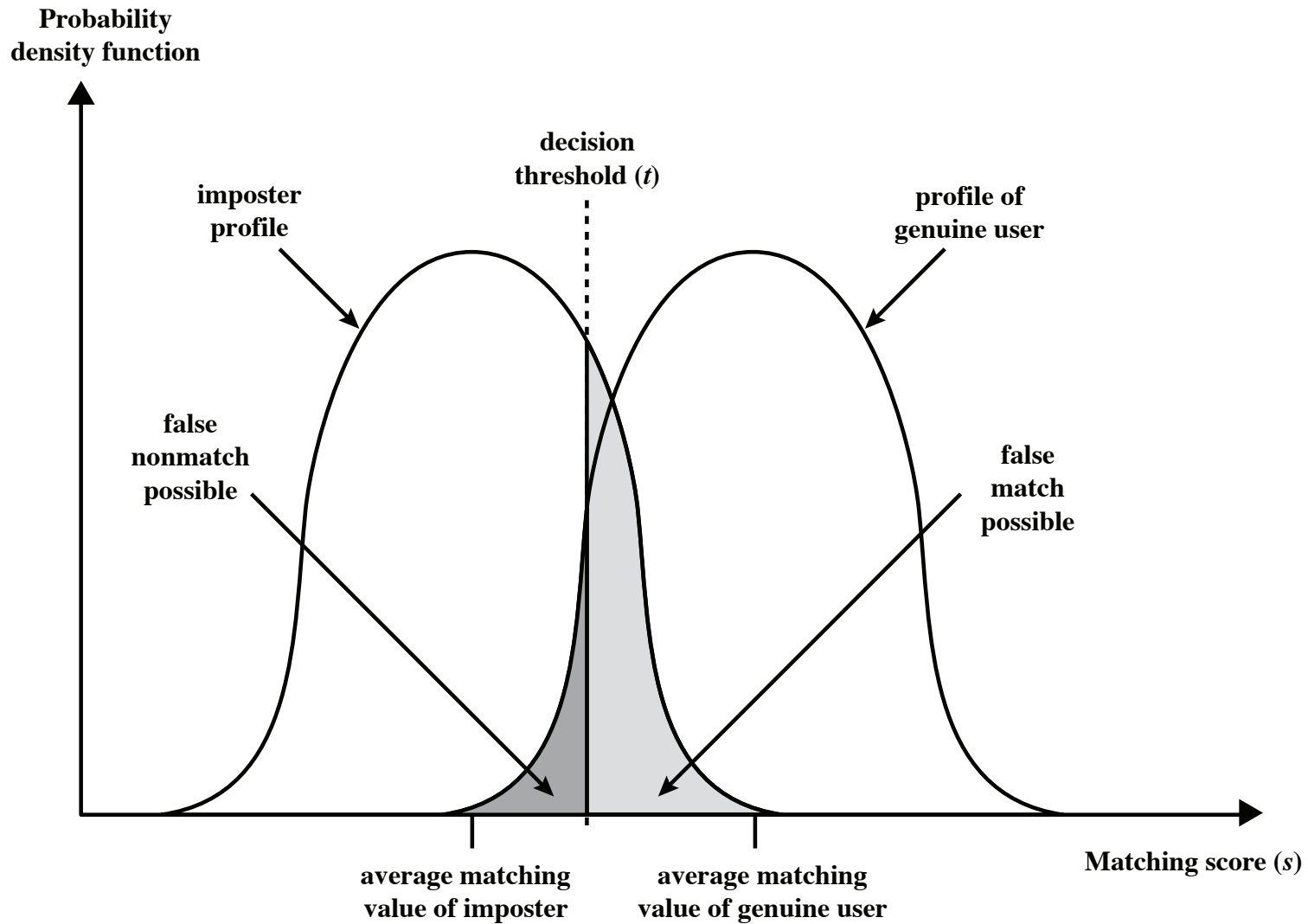


(b) Verification



(c) Identification

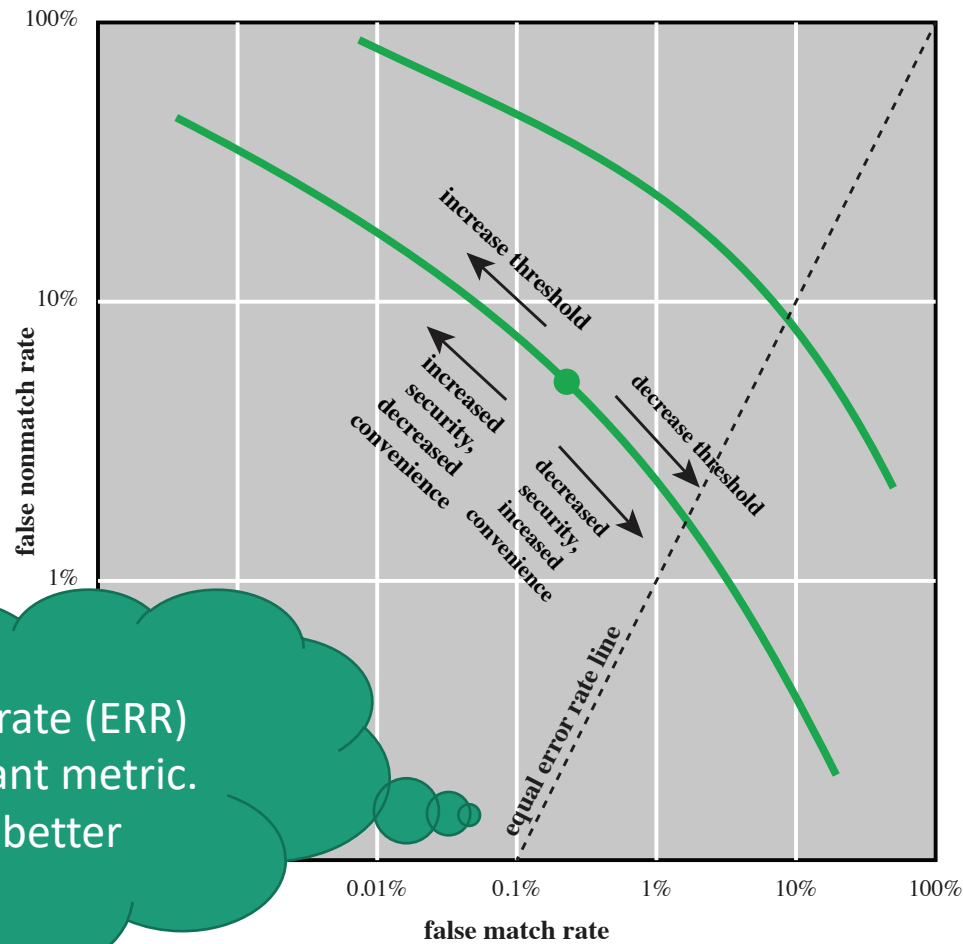
# Probabilistic Identification



# Operating Characteristic Curves

Idealized measurement

log-log scale



Equal-error rate (ERR)  
is an important metric.  
Lower is better

# Actual Measurement

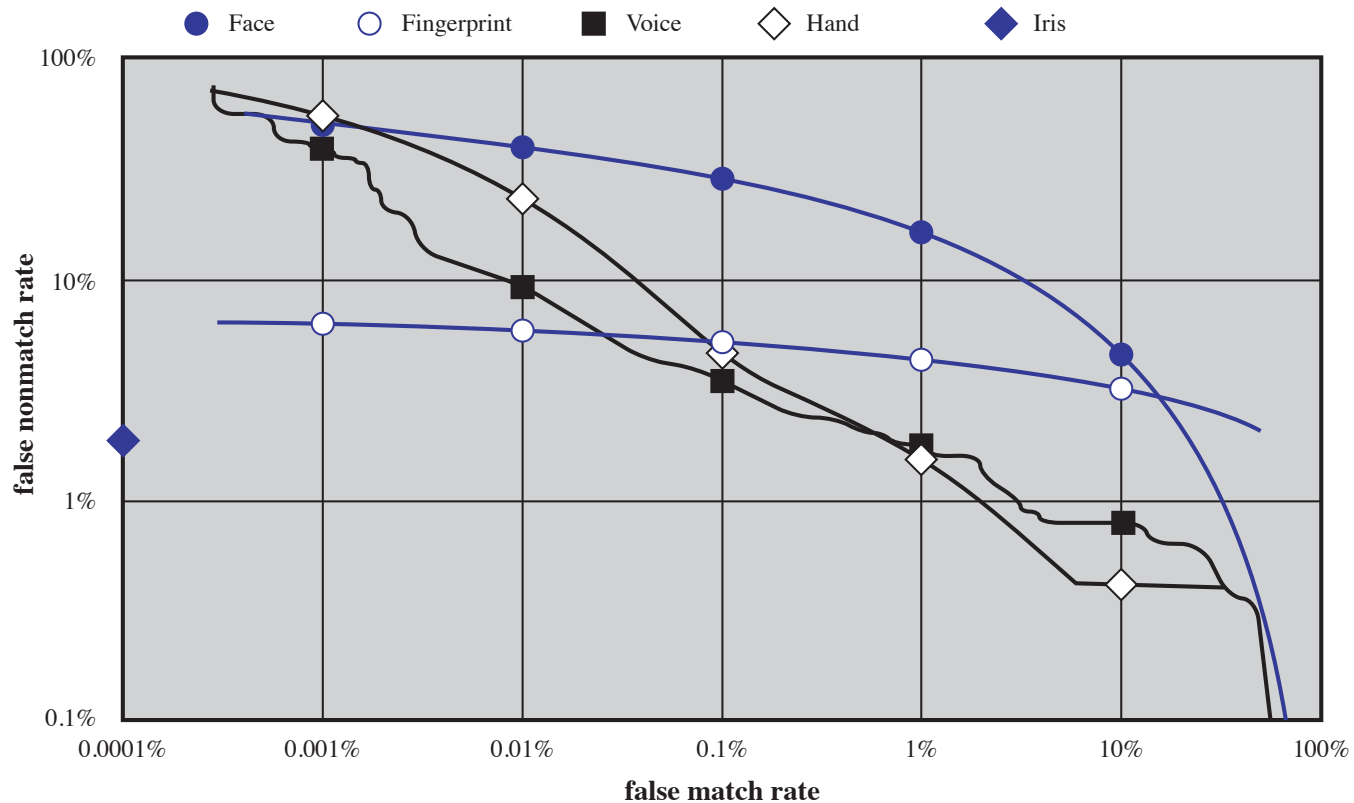
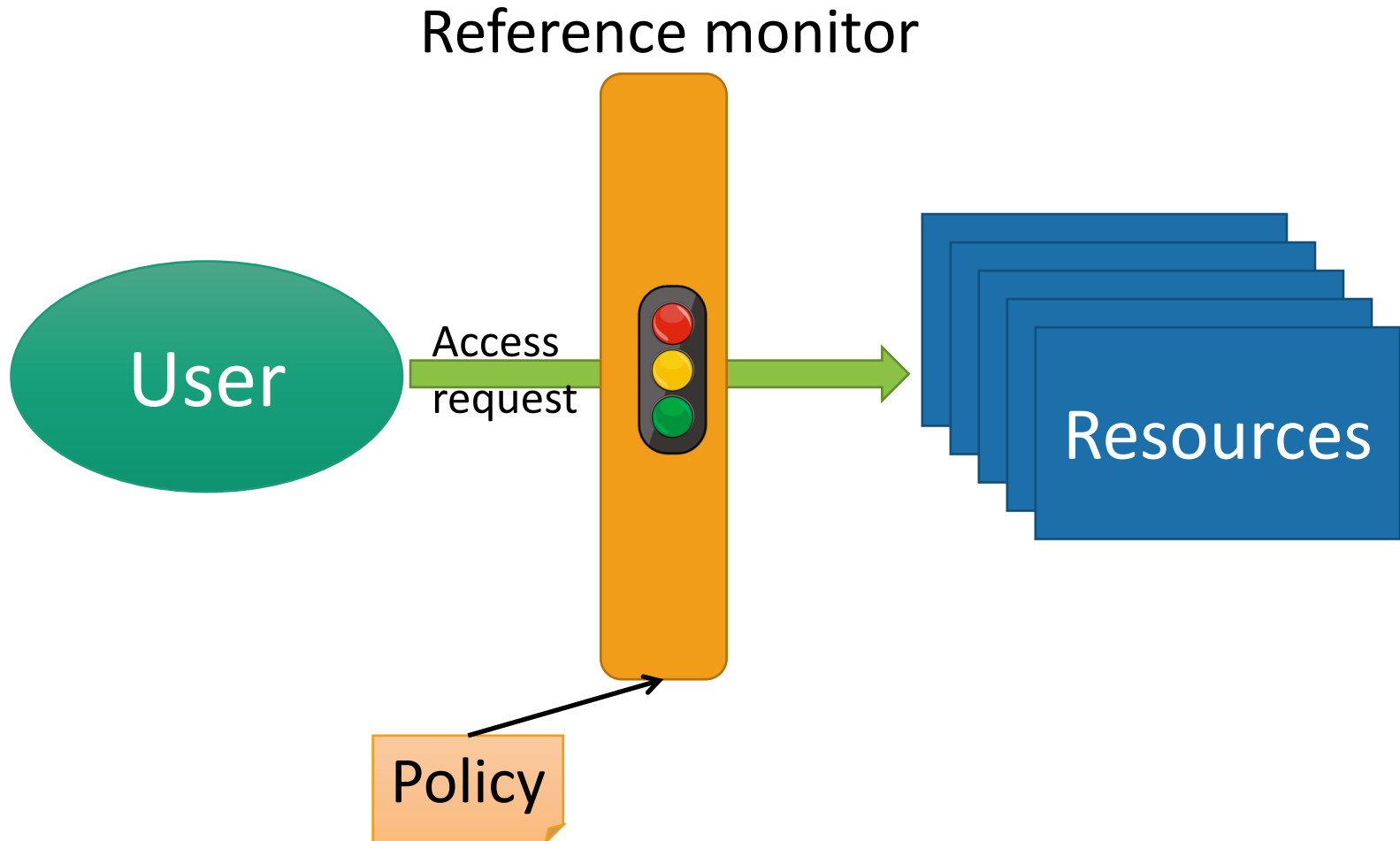


Figure 3.11 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

# Access Control





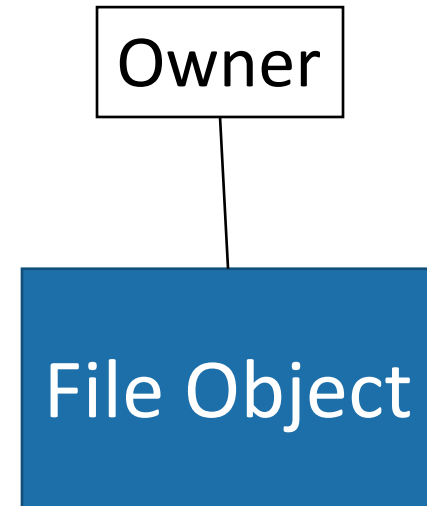
# Access Control Approaches

## Discretionary Access Control (DAC)

- Resources are usually associated with an owner
- Discretionary because the owner can delegate access

## Mandatory Access Control (MAC)

- Operating system or reference monitor strictly manages access
- Access can not be delegated



# DAC Example: UNIX Permissions

Entities

User owner

Group

Others

Resource

File Object

Access

type

RWX

RWX

RWX

# MAC Example: Access control list (ACL)

Resource

File Object

Entity	Access type

- 
- 
-

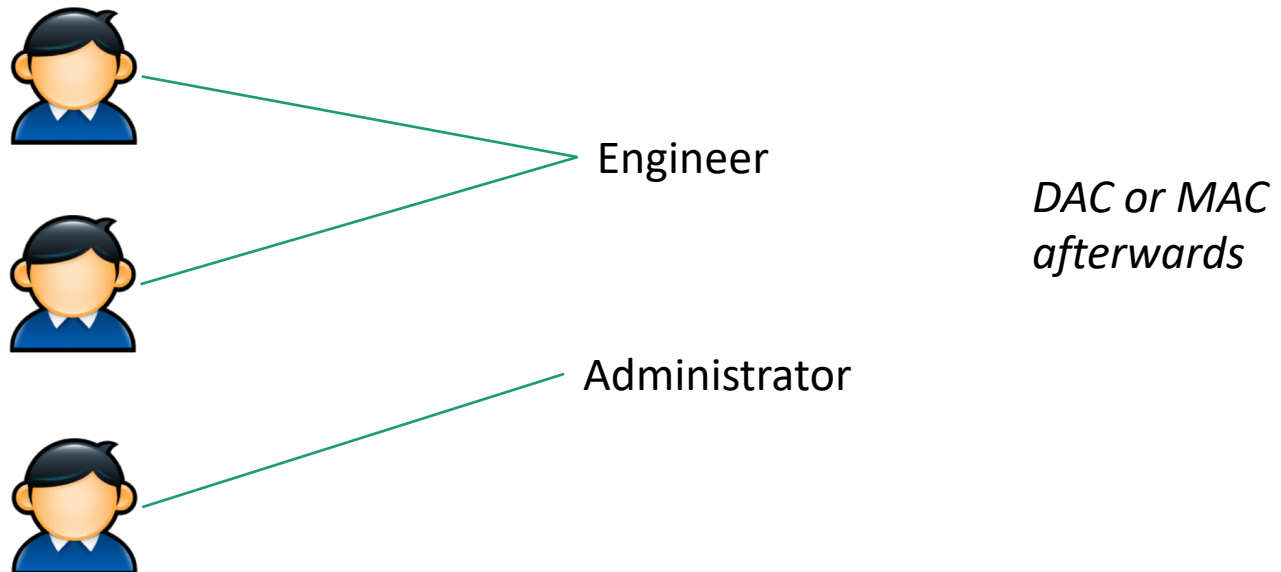
# Role-based Access Control (RBAC)

Policies apply on roles

- Roles are similar to groups

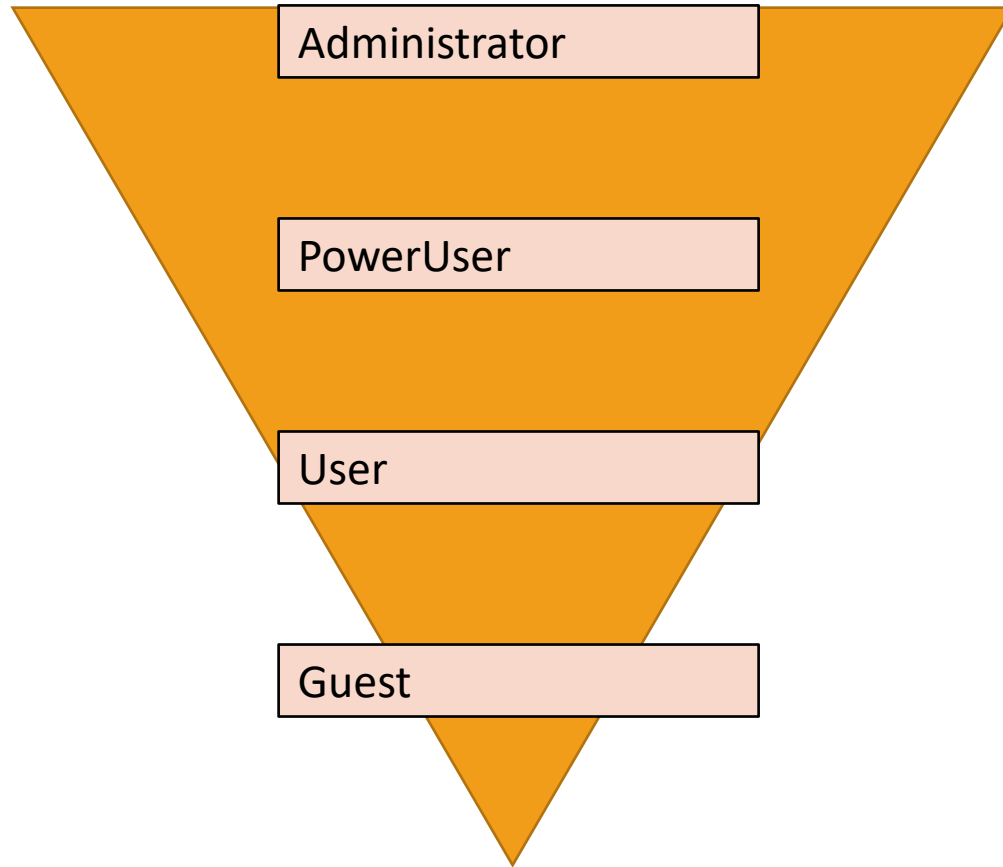
Usually less roles than users → easier management

Easy to handle users switching roles



# Role Hierarchy

More rights



Less rights

# Mix and Match

---

In practice multiple approaches are usually combined to control different type of requests and resources