EECS 3482
Introduction to Computer Security

Access Control

Instructor: N. Vlajic, Fall 2020

Learning Objectives

Upon completion of this material, you should be able to:

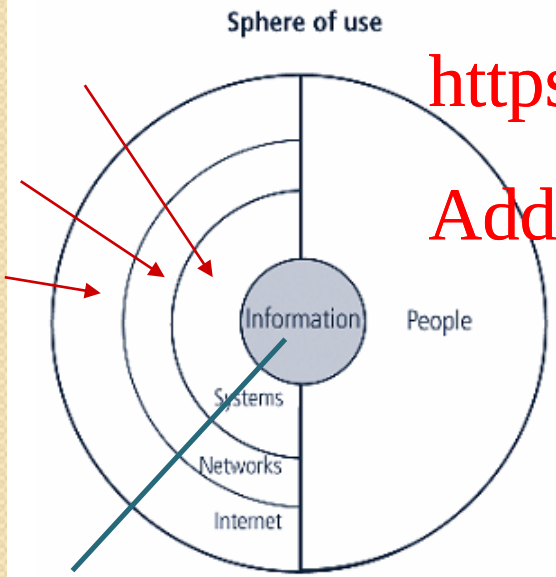
- Discuss three main processes/stages encompassing access control.
- Discuss the four general means of authenticating a user's identity.
- Outline the main pros and cons of various biometric authentication approaches.
- Distinguish between the major categories of access control policies.

Required Reading

Computer Security, Stallings: Chapter 3

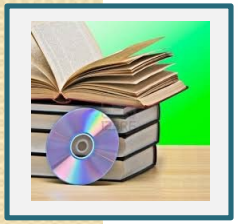
Introduction

- **Spheres of Information Use** – **information can accessed directly** (people accessing hard-copies) **and/or indirectly by means of computer systems**



- **multiple layers on 'technology' side** of access sphere imply that **one or more access stages may be required**

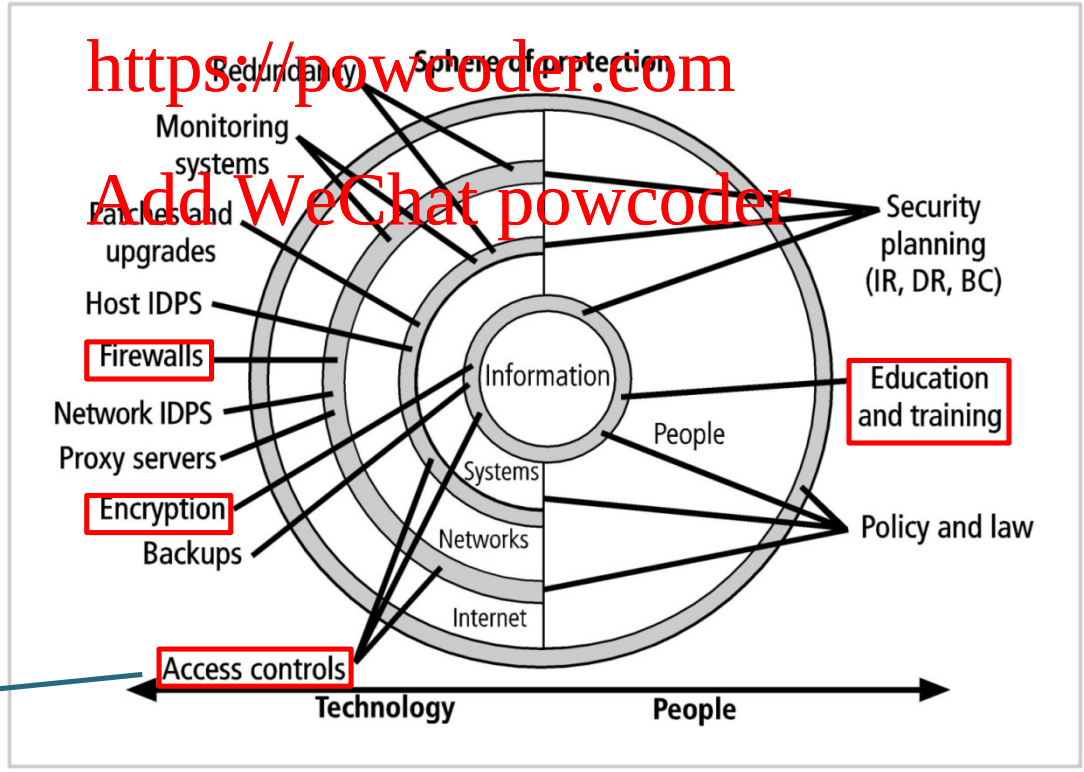
- example: to access info stored on a system (database), the user must access / log-into the database-server
- example: to access info via Internet, the user must 'go through' local network (e.g., pass a firewall) and then access the system that hosts the info



Introduction (cont.)

- **Spheres of Protection** – between each layer of use there must exist a layer of protection to prevent access to next inner layer
  - shaded bands in the figure…

(Avoidance) **controls that can be applied to technology!**



(Avoidance) **controls that can be applied to humans!**

mechanisms that explicitly validate users on 'one by one' basis

Access Control

- **Access Controls** – **selective restriction of access to a physical place, computer system or other resource** (allow only the right/trusted people 'in')
  - **the act of 'accessing' may mean entering, using, consuming …**

Access Control (cont.)

- **Stages of Access Controls**

- **identification** – obtain identity of an entity requesting access to a logical or physical area (obtain credentials)
- **authentication** – confirm identity of the entity seeking access …
  - making sure user's credentials are not false – the user 'is' who they claim to be

- **authorization** – allow the authenticated entity 'in' and determine whether the entity is permitted to access a particular system (OS, firewall, router, database, …) and its resources (e.g., system's files)
  - typically implemented by means of **access control lists / rules**

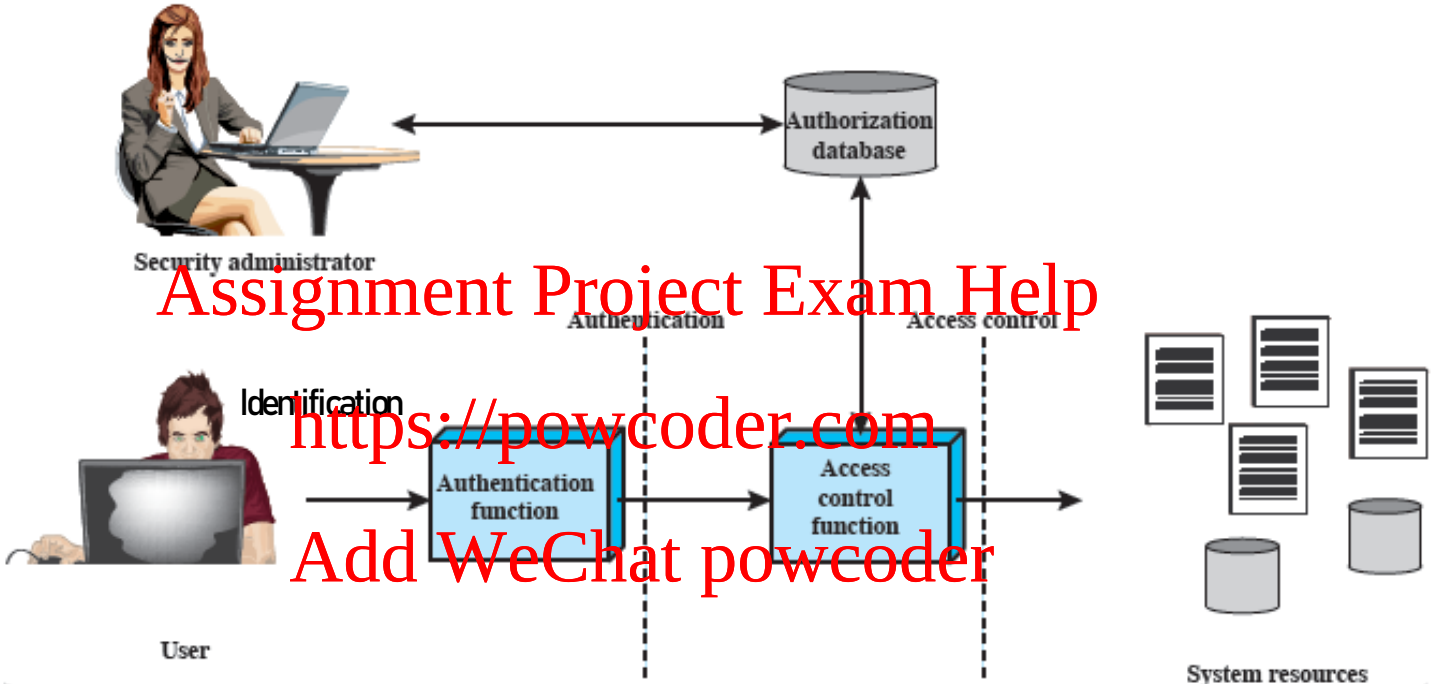
Access Control (cont.)

Example: Basic steps in access control

Action	Description	Scenario Example	Computer Process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Megan reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Megan opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

Table 7-1 Basic steps in access control

Access Control (cont.)



Just because a user can authenticate to a system, it does not mean they are given access to anything and everything.

Authorization ensues that the requested object or activity on an object is possible based on the privileges assigned to the subject.

Identification

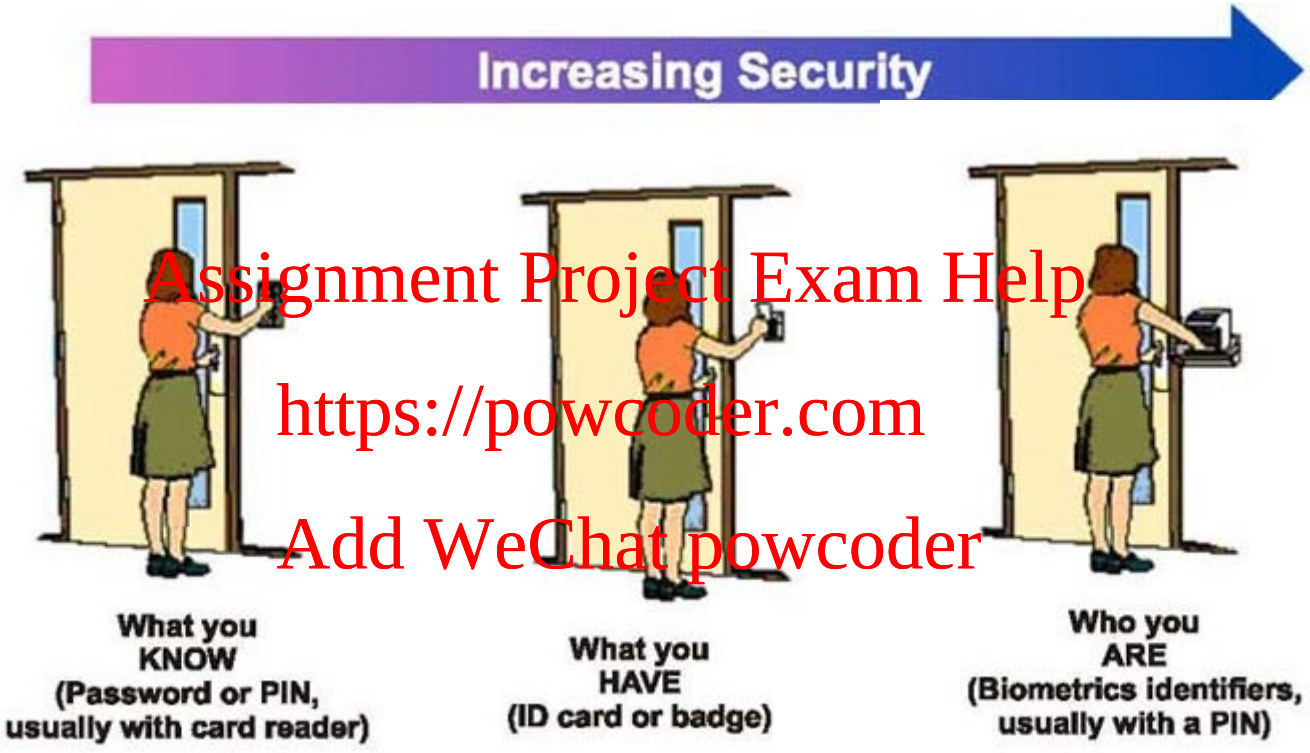
- **Identification** – mechanism that provides info about an **unverified entity** – aka **supplicant** – that wants to be granted access to a logical or physical area
  - identification information/credential must be a **unique value that can be mapped to one and only one entity** within the administered domain
  - in most organizations, identification = surname OR (initial + surname)

Authentication

- **Authentication** – **process of validating a person's (supplicant's) purported identity**
  - **types of authentication mechanisms:**

1) **something you know**
   - password or passphrases
2) **something you have**
   - cryptographic tokens or smart cards
3) **something you are** - static biometrics
   - fingerprints, palm prints, iris scans, …
4) **something you produce** - dynamic biometrics
   - pattern recognition of voice, signature / handwriting, typing rhythm

Authentication (cont.)



http://transit-safety.volpe.dot.gov/security/securityinitiatives/designconsiderations/CD/sec5.htm

If 'something you are' is so much better than 'something you have' or 'something you know' why do not we use biometrics all the time?!

Authentication (cont.)

TABLE 6.1 Examples of authentication techniques	
Example	Factor
Memorized password	Know
Memorized PIN	Know
Magnetic stripe card	Have
One-time password token	Have
SIM card or smart card	Have
USB password token	Have
Fingerprint	Are

Elementary Computer Security, R. E. Smith, pp. 232

Authentication: Something you know …

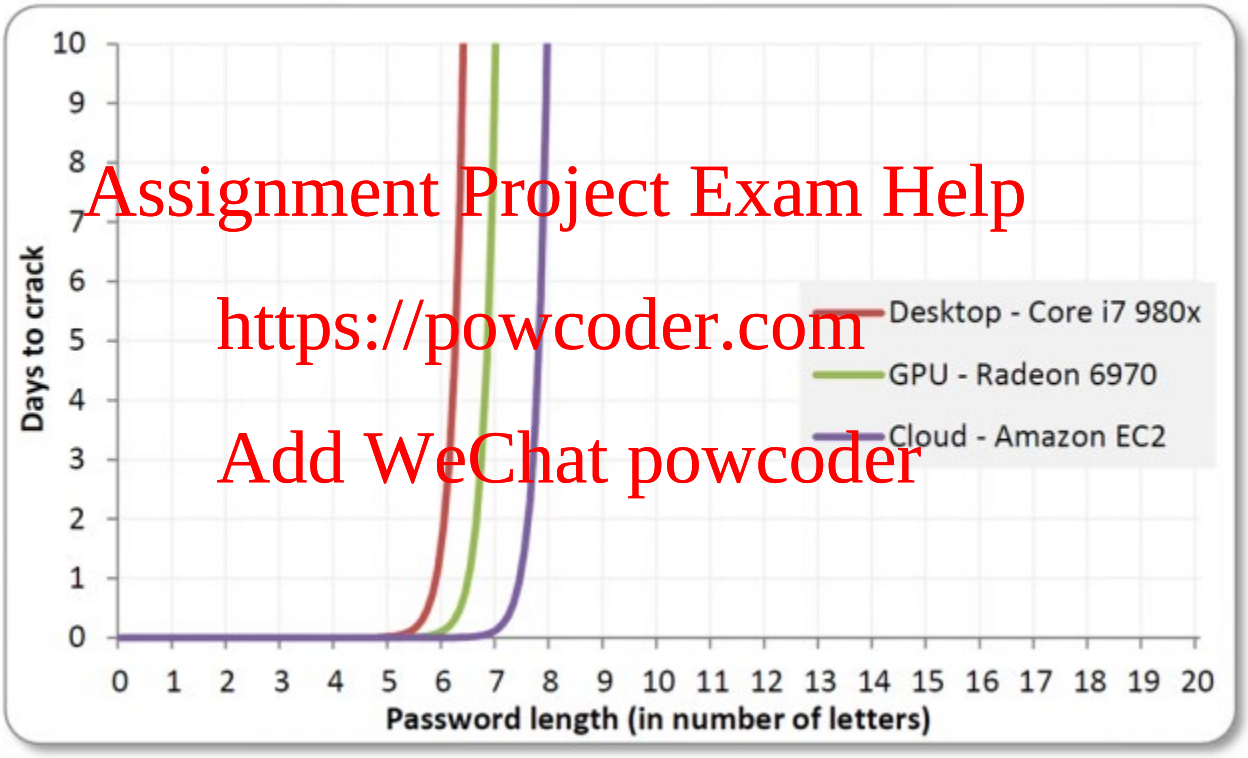
1) Something you know …

- authentication mechanisms based on use of passwords and passphrases
- **password** – combination of characters that only the user should know
  - **challenge**: should be simple enough to remember, and complex enough for cracking
    - bad examples: name of spouse, child, pet
- **passphrase** – plain-language phrase typically longer but stronger than a password, from which a virtual password is derived
  - examples: Linksys, Windows 7 and up

CPIMFF = Cheese Pizza Is My Favorite Food

Authentication: Something you know ...

Example: Password power under brute-force attack (cont.)



http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/2/

The length (# of characters/symbols) in a password is NOT the only thing that matters!!!

Example: Password power under brute-force attack

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

https://cloudnine.com/ediscoverydaily/electronic-discovery/how-long-will-it-take-to-crack-your-password-cybersecurity-trends/

Authentication: Something you have …

2) Something you have …

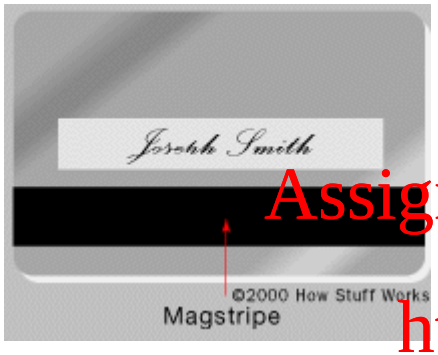
- objects used for purpose of user authentication are called '**tokens**'
- token + PIN/password provides significantly greater security than password alone
  - an adversary must gain physical possession of the token (or be able to duplicate it) in addition to 'cracking' the password

A hacker residing in Australia can 'steel' your password, but he cannot steel your token!

- types of tokens:
  - **static tokens**
  - **dynamic synchronous** (one-time password) **tokens**
  - **dynamic asynchronous** (challenge-response) **tokens**

Authentication: Something you have …

2.1) Static Tokens



- e.g.: swipe card, smart card, RFID tags
- **swipe cards** - ID and ATM cards
  - aka 'dumb cards', transmit same credential every time – the credential (base secret) is impractical to memorize
  - PIN/password not on the card – ATM encrypts PIN provided by user and sends it to a data-base for verification …
- **smart card** - swipe cards with a chip
  - chip contains a CPU, memory blocks (RAM, ROM, …) and on-chip encryption module
  - stores 100x data stored on magnetic strip: encrypted PIN & other info about card holder
  - card checks user's PIN & generates a certificate to authorize transaction process …