

* authentication is the process of ~~defining~~ verifying who someone is.

* authorization is the the process of ~~defining~~ verifying what specific applications, files and data user has access to

chp 5

* What is access control?

a data security ~~technique~~ process that enables organization to manage who is authorized to access corporate data and resources.

- MAC: Mandatory access control $\Rightarrow$ use data classification scheme (predefined set of capabilities and access to information)
ex: who can share what to who

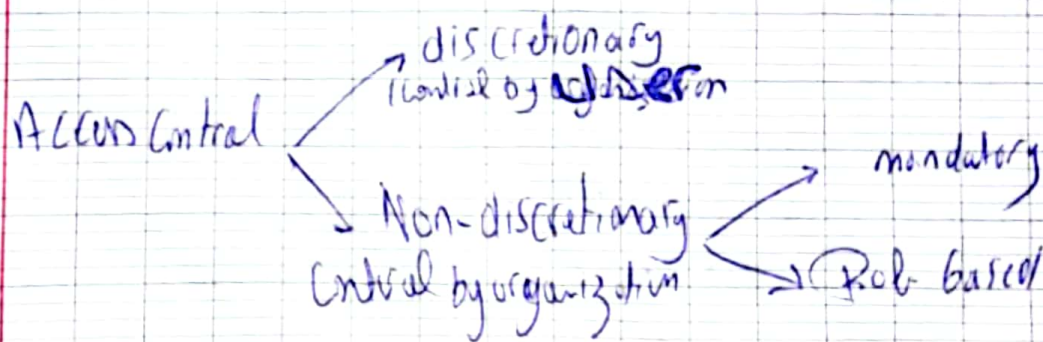
- DAC: Discretionary access control

allow user to control ~~and control~~ and provide access to data/resource at their disposal (user can give access to who they want)
(Because of it's flexibility it can pose a security ~~risk~~ risk to large organization).

- Non-discretionary or role based control: RBAC!

give access based on the organization ^{Access} Role.

enforced version of MAC managed by central authority



2. Content Filter Software Filter (Not Firewall)

allow administrator to restrict content from specific ~~network~~ within a network.

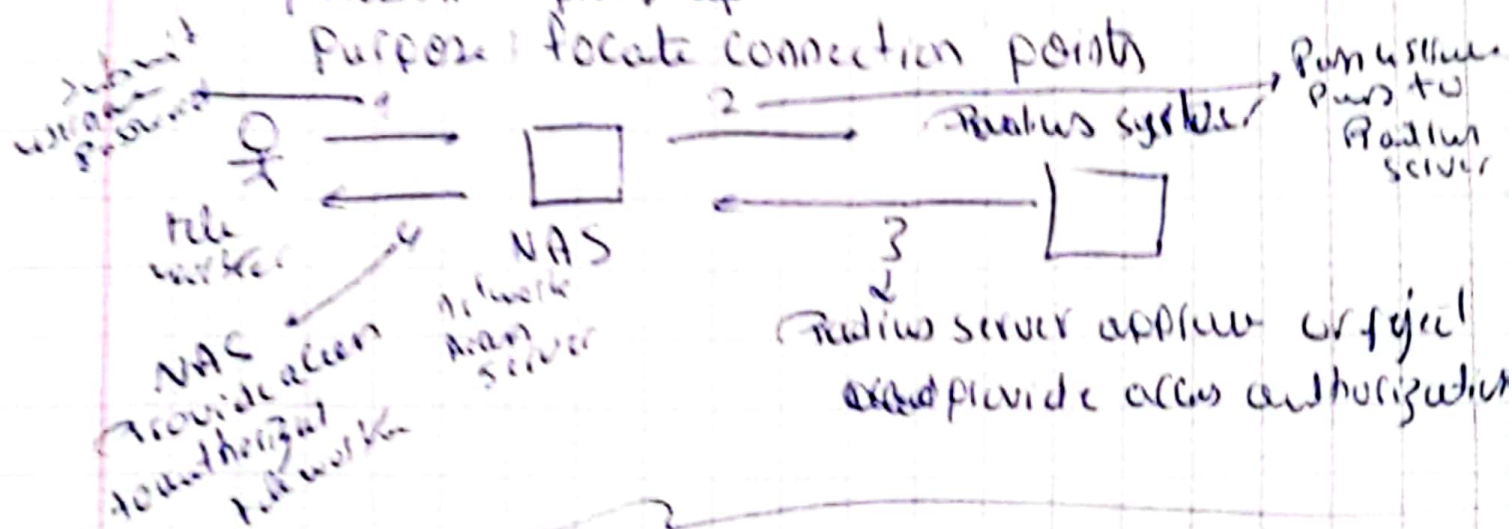
— Primary purpose to restrict internet access to relevant material.

— Most common (restrict from accessing non-business websites or deny incoming spam)

3. Protecting Remote Connections

• using VPNs

• War dialer: automatic phone-dialing program that dial every number in configured range and record no if modem picks up.



RADIUS Server

(improved authentication Poam)

VPNs

Private and secure connection between Sys
Securely extends organizational internal network to remote locations

must accomplish

- Encapsulation of data (incoming)
- Encryption of data (outgoing)
- Authentication of remote computer

turn internet into Private network

Security and Backup technologies

chpt

Fire walls prevent specific type of information moving between networks (restricts internet traffic) computer system or software service or separate network containing supporting devices.

Firewall modes

a) Packet filtering

b) application gateway

c) MAC firewalls

d) hybrid

* Packet filtering firewalls: examine the header info of data packets based on combination of:

- IP Source and destination addresses
- Direction (inbound-outbound)
- TCP (Transmission Control Protocol)

IP	Destination	Service	Action
171.12.X.X	10.10.X.X	ANY	Deny
168.16.X.X	10.12.X.X	FTP	Allow.

* 3 Factors of Firewall architecture

Budget, Objective, Organizational ability.

(available) (for network)

(to develop and implement)

* 4 common architectural implementation of firewall:

- Packet filtering routers, dual-Homed, screened Host, Screened Subnet

router at the boundary between internal and external service provider

manage to reject or allow specific packets

Drawback: Lack of auditing and strong authentication

Page 9

chp 7

Attacks on database:

1) SQL injections

Defenses against:

check input users (golden-rule
all inputs are evil)

Using SQL malicious code to get
unauthorized access
For example: `select * from where Login = '1' 1=1`

`select * where city = 'Redmond'; Drop Table`

2) Inference attacks: (استنتاج)

For example when there is only one girl in specific class:

`select * from class where gender = "Female";`

- Defenses:

- Do not allow aggregate query result when set of tuples selected are too large or too small.

- Transform data by ~~transforming~~ ^{removing} identifying info.
 → Deidentification
 → An organization has to be done with care.

Encryption:

- Last line in defense in Database Security

- Can be applied to the entire database at record level, ~~at~~ attribute level and individual file

Disadvantages:

- Key management (Authorized users must have access to decryption key)

- Inflexibility (when all data base is encrypted it becomes hard to perform other searching).

Token based authentication: object that user possesses for the purpose of user authentication. ex: ATM Tokens.

chp 6.8 why securing data stored in data base is so important and different?

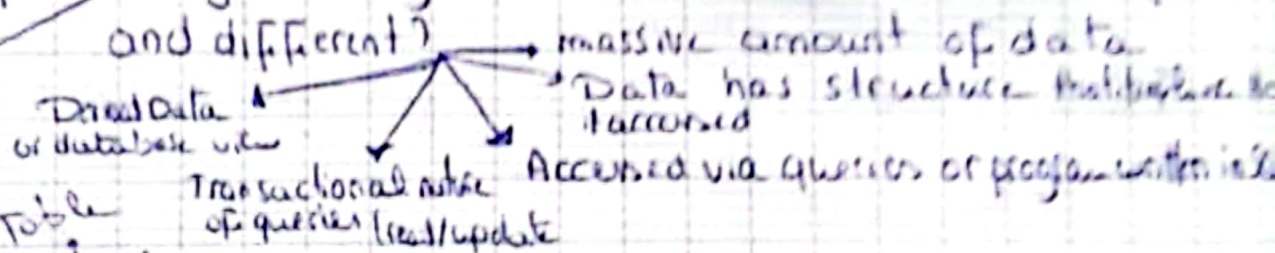


Table 1

attributes	ID	Name	Salary
Tuples	1	SMN	#22
	2	RAM	#33

• Key used to access data in tuples

• a table is defined by schema

* Operation in relations: create, select, insert, update, delete

Example: Select * from Employee where DID = 15

• we can preclude ~~data~~ sensitive attributes that should not be accessible to certain users so we can use database view to enhance security.

* Database access control has 2 commands: Grant, Revoke

Grant {privilege/role?} ON table TO {user/role/public?} [identified by Password] [with grant option]

Example: GRANT SELECT ON ANY Table TO ALICE

Revoke {privilege/role?} ON Table FROM {user/role?}

Example: REVOKE SELECT ON ANY Table FROM ALICE public

• Revoking access only affects the direct grantees, not who receive access through subsequent grants (when ALICE revoke access from BOB, charlie access remains)

identification: unverified entities seeking access to a resource provide a label which they are known to the system. (unverified entities wanting access to the resource offer an identification number to identify themselves to the system.)

Password

Passphrase (series of characters typically by the user)

Smart Card: ID or ATM: with magnetic stripe

Smart card: (contains a computer chip)

Authentication Factors

Synchronous tokens

asynchronous tokens

Authorization can be handled in 3 different ways:

For each user

For member group

action multiple systems.

Accountability (المسئولية):

ensure that all action on a system - authorized or unauthorized - can be attributed to an authenticated user

accomplished by system logs $\Rightarrow$ record specific info (how many users)

Access control matrix:

	x	y	z
A	rx	r	
B		rw, rx	
C		rw	rx

1) ACL (Access Control List for columns)

$x \rightarrow [A, rx]$

2) C-Lists (Capabilities lists for rows)

$y \rightarrow [A, r] [B, rw] [C, rx]$

$z \rightarrow [B, rw] [C, rx]$

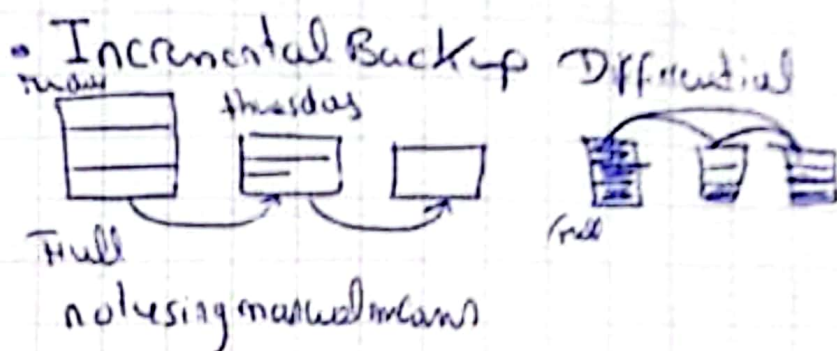
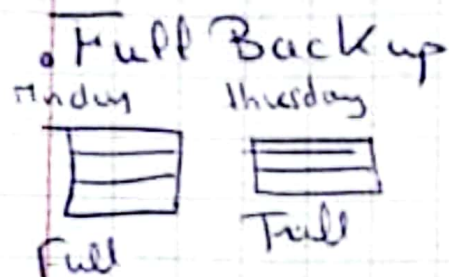
$A \rightarrow [x, rx] [y, r]$

$B \rightarrow [y, rw] [C, rx]$

$C \rightarrow [y, rw] [C, rx]$

3-2-5, Backup Strategy
 Strategy: 1- At least 3 copies of your data or Backed up data in 2 different storage
 3 - at least one copy of data off site

2) Backup



Backup tech: RAID (Redundant Array of Independent Disks)

Redundancy	RAID 0	RAID 1	RAID 2	RAID 4
present data	A ₁ A ₂	A ₁ A ₁	A ₁ A ₂ A ₃	A ₁ A ₂ A ₃ A _p
	A ₄ A ₄	A ₂ A ₂	B ₁ B ₂ B ₃	B ₁ B ₂ B ₃ B _p
	A ₅ A ₆	A ₃ A ₃	B ₄ B ₅ B ₆	B ₄ B ₅ B ₆ C _p

Stripping Mirroring Stripping + parity

data storage virtualization technology
 combine multiple physical disk drive
 components into 1 or more logical units for the purpose
 of data redundancy performance
 improvement

Cloud Data Backup:

data on business servers are backed up into a remote server.

5 common Backup mistakes:

- 1 - Not doing backup
- 2 - Saving the Backup copy on the same Hardware as original file
- 3 - Not testing the Backup
- 4 - Not Running the Backup regularly and sufficiently frequently
- 5 - Not Labeling Backup files.

6) Port Scanners

- used by attacker and defender to identify fingerprint computers active on a network and other useful info
- more specific more useful

7) Firewall analysis tools:

discovery of firewall rules and assist in analyzing the

8) Operating Sys Detection tools.

once OS is known $\Rightarrow$ attacker can determine vulnerabilities

9) Vulnerability Scanner:

Active vulnerability Scanner: Highly detailed info

Passive vulnerability Scanner: identify vulnerable version of both server and client software.

10) Packet Sniffers:

Capture copy of packet and analyze it.

Provide valuable info for diagnosing and resolving networking issues.

- can be used to eaves drop

11) Wireless Security tools.

Security Breach if you didn't secure it wireless.

Assess the level of privacy or confidentiality.

12) Backdoor

Active response:
Taking action against intrusion
IDS can generate reports, routine

Passive response:
Setting off alarms.

3 Basic control strategies for IDS:

Deploying
Planning

- Centralized: all functions are implemented and managed in central location
- Fully distributed: applied at physical loc of IDS
- Partially distributed: combine 2 & agent can still analyze and respond to local threats, they report to a Hierarchical central facility.

NIST recommend 4 loc for NIDS sensors:

- Loc 1: Behind each external firewall. in Network DMZ
- Loc 2: outside an external firewall.
- Loc 3: on major network backbones
- Loc 4: on critical subnet

Host based IDS:

Deploying Host based IDS:

- o implement most critical software
- o all systems installed w/ org reach planned degree of coverage.

5/ Scanning and Analysis tools:

OS used to collect information needed to launch an attack

Foot printing: collecting publicly available info about target
Fingerprinting: reveal useful info about internal structure and nature of target system

Attack protocol: sequence of protocols and steps used by an attacker to launch attack against system

Valuable to network defender?
can quickly pinpoint part of system that need a

4. Intrusion Detection and Prevention System :

- Intrusion detection consists of procedures systems to identify detect
 - Intrusion Prevention activities that deter intrusion
 - Intrusion Reaction encompasses of action regulation under take when intrusion detected
 - Intrusion Correction : Complete Restoration of operation to normal state (identify source and method of intrusion)
- Intrusion detection systems: detect violation and activate alarms.

Why we use IDS? (like crack...)

- Purpose : identify-report intrusion
- Prevent-mitigate loss-damage ~~of~~

* Data Collection (what Happened after intrusion and
* quality assurance and continuous improvement.

Type of IDS:

Network Based
(protecting network information)
exam traffic flow on a network in an attempt to recognize abnormal patterns.

Host Based
Resides on particular computer and monitor activity in system

IDS methods :

- Anomaly based detection : collect summaries by observing traffic to be normal. when measured activity is outside baseline parameters. IDS send alerts to administrator.
- Logfile monitors.
Review log file generated by server, network devices or other IDS system for patterns and signature.

2/18) Cryptology: Science of encryption; combining cryptography and cryptanalysis.

Cryptography: process of making and using code to secure transmission of info.

Cryptoanalysis:

process of obtaining original message from encrypted message without knowing algorithm and key used to perform encryption.

- Encryption: Converting original message into readable by an authorized user

- Decryption: Converting from ciphertext to plaintext

- Algorithm: mathematical formula used to convert unencrypted message into an encrypted

cipher: transformation of the individual components (byte, character) of an unencrypted message to encrypted components.

- Ciphertext or cryptogram: The encrypted or encoded message result from encryption.

- Decipher: Decrypt ciphertext to plain

- Encipher: encrypt

Key or crypto variable: info used in conjunction with algo. to create ciphertext.

Plaintext: unencrypted msg

Steganography: Process of hiding in picture or graphics.

PKI protect info assets in several way.

authentication: validate the identity of others.

Integrity: Content signed by certificate has not been altered

Privacy: keep info from being intercepted

authorization: enhance security, controlling access privacy

non-repudiation: less likely to repudiate a digitally signed transaction.

Digital signatures

why created? to verify info transferred using electronic system

Created using Asymmetric encryption

To verify authenticity

digital signature = authentication tag of message

Computed by one verified by many.

Hybrid Cryptography systems:

X Diffie-Hellman key exchange:

way to exchange key without exposure to third party.

use asymmetric encryption to exchange symmetric key.

Cryptanalysis:

to retrieve keys not just msg.

Brute force attack

Try every possible key until it works
of ciphertext until it works

Brute force Search:

• try every key

• proportional to key size

authentication
integrity
Non-repudiation

Hash Function: Data Integrity and Source Authentication

• Encryption does not protect data from modification from another party.

we need a way to ensure that the data arrives at destination in its original form, and it's coming from authenticated source.

— Mathematical ~~function~~ algorithm that generate message summary known as message digest.

— Convert into fixed length msg (no key use in Hash)

ex. used in password verification to confirm identity of users.

Fox — cryptographic hash function —> DFCD ABCD EFGH

Andis Smart — 1.1 —> 5D10 0BCD 10AC

* Message Authentication Code (MAC)

MAC scheme is Hash family, used for authentication.

(the sender and receiver share a key).

Same MAC should be found

* Public Key Infrastructure (PKI)

Integrated system of software, encryption methodologies, protocols, legal agreement, third party services. Enabling users to communicate securely.

Cryptosystem

* Rowtransposition Cipher:

Plaintext: A H M A S T A S L B N N $\Rightarrow$

	1	2	3	4
1	A	H	M	A
2	O	T	A	S
3	L	B	N	N

Key: 4 3 3 2
 encrypted: A S N A O L H A N H T B

* H = COUNT THE COST $\Rightarrow$

	1	2	3	4	Key		1	2	3	4
1	C	N	H	O		H	O	C	N	
2	O	T	E	S		E	S	O	T	
3	U	T	C	T		C	T	U	T	

Key = 3 4 1 2
 enc = C = H O C N E S O T C T U T

* Product Cipher:

- Vernam Cipher (one-time pad)

A	B	C	D	E	F	G	H	K...	Z
D	1	2	3	4	5	6	7	8	25

MSG: I S M A I L $\Rightarrow$ 8 18 12 0 8 11

Key: A B C D E F $\Rightarrow$ 0 1 25 2 3 6

$(8) (19) (31) (2) (11) (13) = \boxed{ITLC P}$
 $\downarrow$
 $31 \bmod 26$
 (11)

Cryptographic algorithms

Symmetric

Asymmetric

distinguished by type of keys.

Same key for cipher/decrypt

- o minimal processing
- o both sender & receiver must possess encryption key
- o DES (DATA encryption Standard)
- o 3DES (triple)
- o ADVANCED encryption Standard

- o different but related keys
- o if key A encrypt only key B can decrypt
- o One serve as private key (known owner of the key (pair) other serve as public key.
- o 4 keys to hold single comm between 2 parties

Bit stream = each plaintext bit transformed into cipher bit one bit at a time

Cipher methods $\rightarrow$ Block cipher
 stream = message divided into blocks and each transformed into encrypted block

$$E(M) = C$$

$$E(M, K) = C$$

$$D[E(M)] = M$$

The most commonly used algorithm include 2 functions:
 Substitution and transposition

* Substitution cipher: (substitute one value with another)
 very powerful if combined with other ops

Arabic $\downarrow$ Polyalphabetic (A $\rightarrow$ BC or BCD)
 Vigenere cipher (invented from poly)

Caesar cipher: 3 values shift to the right.
 replace each letter by 3rd letter on
 MEET $\rightarrow$ PHHW

A	B	C	D	...	2
A	A	B	C	D	...
B	B	C	D	E	...
C	C	D	E	F	...
D	D	E	F	G	...
...	...	...	...	...	...
2					

Text to encrypt: ISHAEL
 Key: LEMON
 ISHAEL
 LEMONL

encrypt text: TWYOVW
 cipher

if you want to shift more than 3:

a	b	c	d	e	f	g	h	...
0	1	2	3	4	5	6	7	...

$$C = E(P) = (P + K) \bmod 26$$

$$P = D(C) = (C - K) \bmod 26$$

$\rightarrow$ decrypt $\rightarrow$ nb to be shifted index of character

- Transposition cipher:

Rail Fence cipher: write letters out diagonally over nb of rows then read row by row

Message: ISHAEL KPHAR

write as: I H I K T A

S A L A T R

in cy: IMIKTASALATR