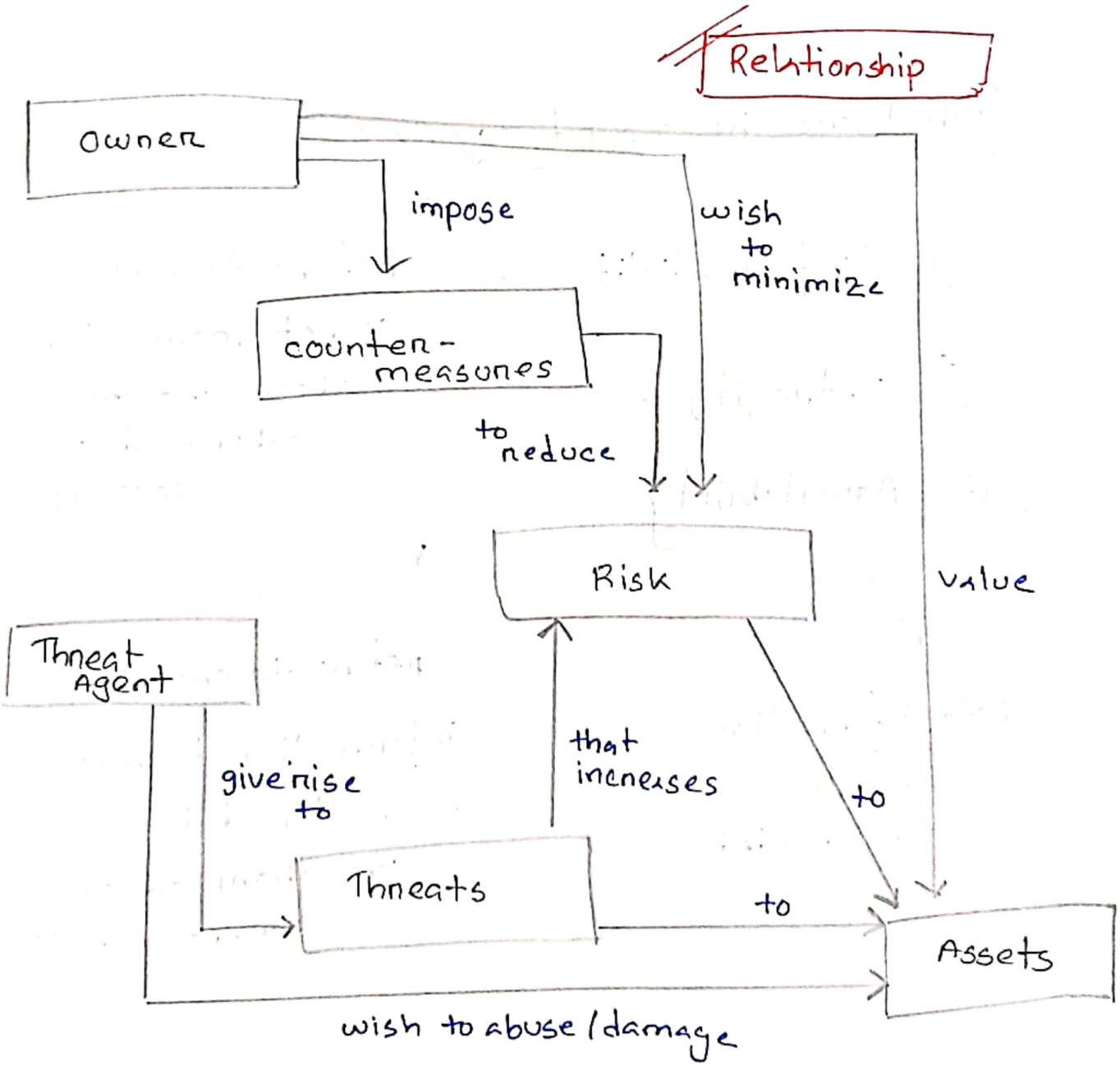
what is common criteria (cc)?

→ cc is a set of guidelines that provides a framework for evaluting and certifying the security features and capabilities of IT product and service.



what is security?

→ refens to within systems, application, protocols relies on specfic properties intend to prevent unauthonized access, alteration, destruction, disruption.

what are the security goals?

1. Confidentiality → refens to keeping info. secret from all but those who are athonised can access it

what is confidentiality

2. Intregity

what is Intregity

refens to ensuring information hasnot been altered by uncuthonized or unknown means

3. Availability

Data/ information is available when needed

what is availability

Q. with respect to the C.I.A and A.A.A concept what risks are posed by Trojan Horse?

TH

Final-17

(1) confidentiality :-

TH allows unauthorize access to sensitive info. disquised as legitimate software. can steal or copy confidential data without user knowledge

Intregity;- data and system are compnomised due to TH. modify, délete data, alter system configuration

Availability : impact the availability of system/networks. by consuming system nesource or disrupting network operation

make system unavailable to usen .

Confidentiality

Two dimmension

what is Secrecy ?

Secrecy is about keeping sensitive information hidden from people who shouldn't have access to it

(protection from unauthonize)

what is privacy ?

privacy is about having control over your personal information and deciding who gets to know what about you

(protecting personal info)

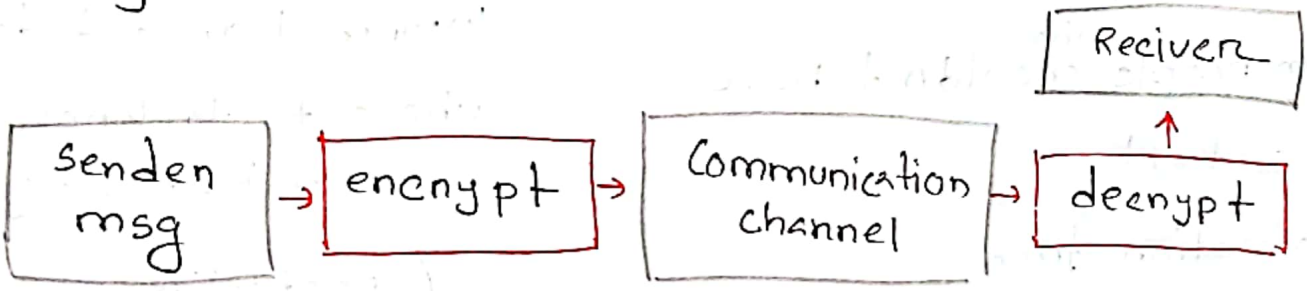
what are Tools of confidentiality ?

5 tools

1. Encryption
2. Access control → limiting access using Roles and policies
3. Authentication
4. Authonization
5. physical security

what is encryption?

→ is the process of transformation of information using a secret key called encryption key and the transformed information can only be read using another secret called decryption key.



Authentication vs Authonization

① who are you?	① what are you allowed to do?
② is the process of verifying the identity of a user or entity.	② is the process of determing what actions or resource a user is allowed to access or perform after they have been authenticated.

Intregity

two dimmension

what is data Intregity?

→ means keeping info and prognam safe from any changes unless theyne allowed and appnoved

what is system Intregity?

→ is like making sune a computen/ system does its job propenly without any unwanted interfenence

what ane tools of Intregity?

1. Backups
2. checksoms →
3. Data connecting codes

what is checksum?

a checksum is a simple way to check if a file has been changed on connupted.

(a checksum function depends on the entine content, a small change to the file will nesult in a diffenent output value.)

what are the security properties? 6 prop-

1. confidentiality
   - Encryption
   - Access controll
   - Authentication
   - Authorization
   - physical security
2. Integrity
   - Backups
   - checksum
   - Data connecting codes
3. Availability
   - physical protection
   - compotional Redundanices
4. Authenticity → The property of an entity on source of data being geniune and being able to verified & trusted
5. Accountability
6. Anonymity → :- refers to the condition where certain records/actions /transaction cannot be directly linked to any specific Individual.

(*) Difference between passive and active security attack?

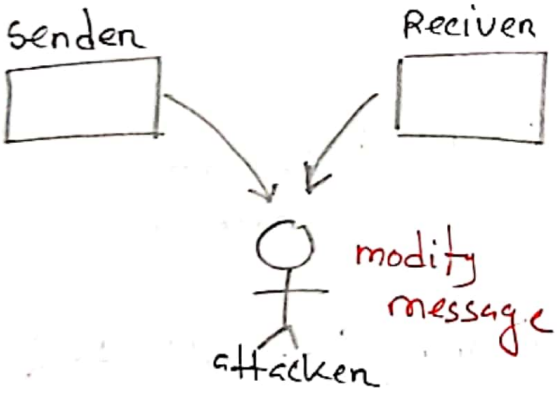
Active attack	Passive attack
(1) Active attack is danger to Integrity & Availability	(1) danger to confidentiality
(2) modification information takeplace	(2) no modification
(3) attention is on prevention	(3) is on detection
(4) due to this attack, execution is always damaged	(4) no harm to system
(5) system resources also canbechanged	(5) no change in system resource
(6) can easily detected	(7) very difficult to detect
(7) purspose is to harm the ecosystem	(7) purpose is to learn about the ecosystem

(8) duration :- short

(9) Complexity :- High

(10) def :- what is active attack?

Active attack is an attack where the attackens attempts to modify / alter the content of message on the system itself



(11) Type

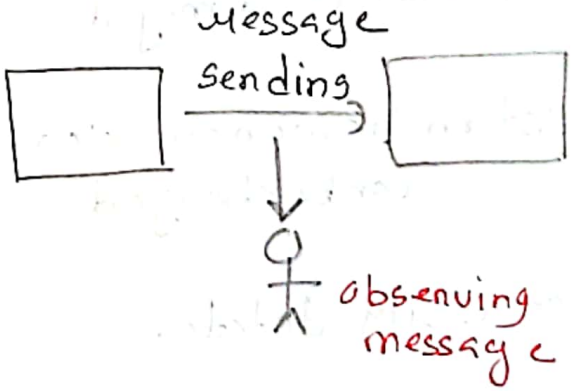
1. Dos
2. Modification
3. Masquenade

(8) duration :- long

(9) complexity :- low

(10) def :- what is passive attack?

passive attack is an attack that involve the attacken observing / monitoring the system without making any changes to it

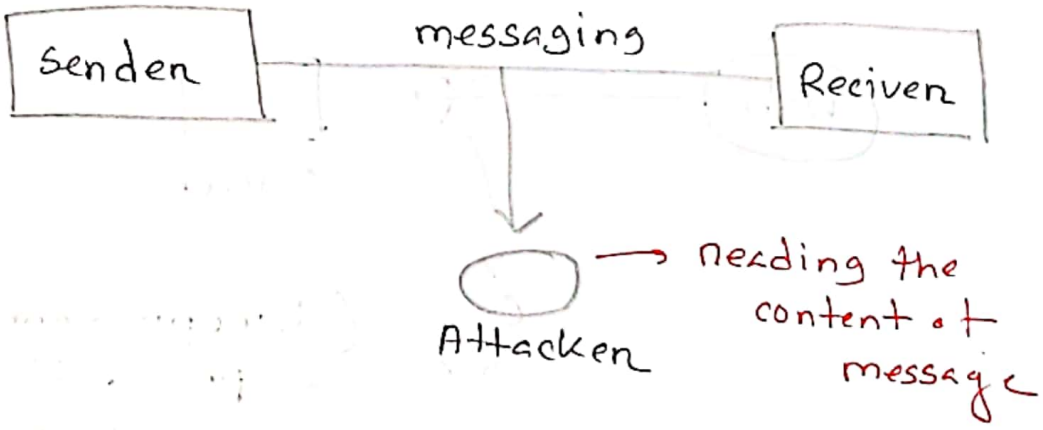


(11) Type :-

1. Eaves eyedropping
2. Traffice analysis
3. Replay

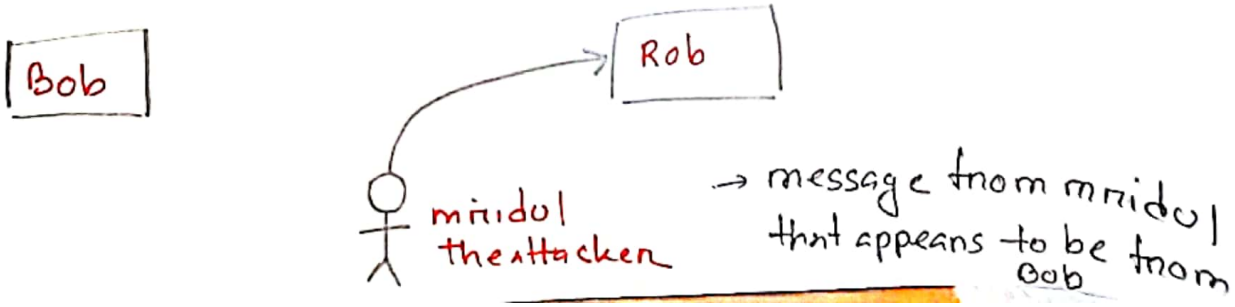
(*) what is Eaves dropping Attack?

→ It is passive attack where attackers intenecpts and neads data that is transmitted between two device without the knowledge or consent of the panties involved.



(*) what is masquenading Attack?

→ it is a type of active attack whene attackens pretends to be someone else (a legitimate user/system) to gain unauthonized access to system / data.



what is Dos attack?

→ Denial of service is a type of active attack where attackers aim to render a computer/device unavailable to its intended users by interrupting the device's normal functionality.