UNIT-I

INTRODUCTION & NUMBER THEORY :-

UNIT-I

Basic terminology:-

Cryptology:-

* Cryptology is the study of techniques for ensuring secrecy & authentication of information.

> Cryptography - study of design of techniques.

> Crypt analysis - This deals with the concept of defeating cryptography.

* Network security:-

It covers the use of cryptographic algorithms in network protocols and n/w appln.

* Computer security:-

Refers to the security of computers against intrudees & malicious s/w.

*. Information security:-

Information needs to be secured. The security of info needs to be against physical damage & administrative damage.

*. Computer Security :-

* It is the collection of tools to protect data & thwart hacker is called computer security.

*. Network Security :-

Used to protect the data during the transmission across the n/w.

*. Internet Security :-

Security against the data when it transmitted across the I/n.

*. OSI Security Architecture :-

* OSI architecture provides a systematic way to organize the security.

> Security Attack
> Security Mechanism
> Security Service.

Threat :- It is a possible danger that exploit vulnerability.

Attack :- It is an intelligent act (ie) deliberate to evade security & violate the security policy of a system.

* Security Attack :-

* Attack is defined as an action that compromises the security of info owned by the org.

* It can be classified as,

> passive attack

> Active attack

* Passive attack :-

* the opponent wants to obtain the info is being transmitted across the n/w & involves no alteration.

Characteristics :-

> Difficult to detect

> Possible to prevent by encryption

classification :-

* Release of message contents :-

* The msg to be transmitted should be prevented from eaves-dropping.

> Traffic Analysis

* Here, the intruder watches the frequency, length of msg exchanged blw the two principals.

* Active Attacks :-

* Involves alteration to the

Characteristics :-

> Difficult to prevent

> Detection is feasible. & can be recovered from the causes.

classification :-

> Masquerade

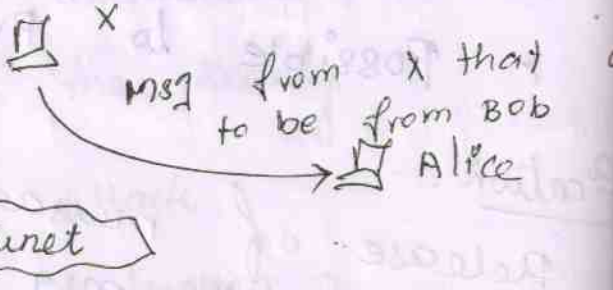
> Replay

> Modification of msgs

> Denial of sevice.

> s/w attack.

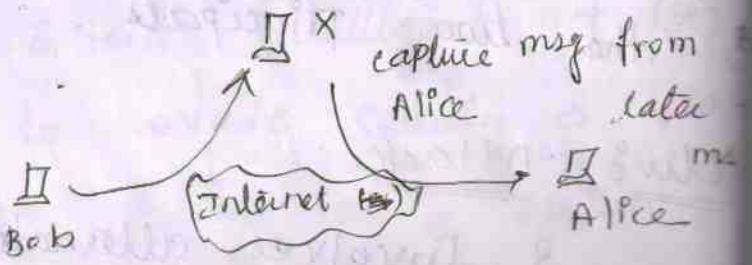
* Masquerade :-



*. when one entity prelends to b a different entity.

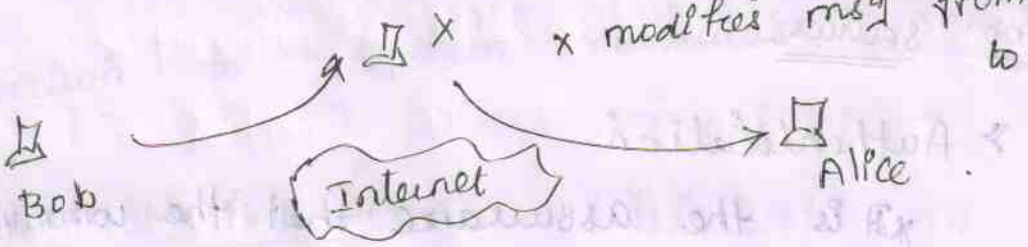
*. the attacker captures the au -tion & impersonifies the sender.

* Replay :-



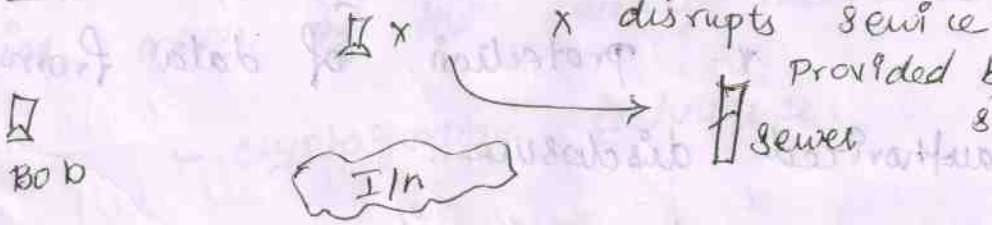
* the attacker captures the msg & retransmits the msg without any modification to produce unauthorized effect. (6)

* Modification of messages :-



* The attacker captures the msg & retransmits the msg with modification (or) delays (or) reorder the msg to produce unauthorized effect.

* Denial of service :-



Attack has specific target like supress all the msgs directed to a user (or) disable the n/w, degrade the performance.

* Slow Attack :-

x. Slow attacks are those which can be introduce into the systems (or) n/ws. Ex: worms, viruses.

Security services :-

X800: * Security sewice is a sewice p
by the protocol layer, which ensures s
of the systems (or) data transfer.

X.800 services :-

> Authentication

* It is the assurance that the comm
entity is the one that it claims

> Access control

* the access control is the p
of unauthorized use of a resource.

> Data confidentiality

* protection of data from
unauthorized disclosure.

> Data Integrity

*. This gives the assurance tha
data received are not modified / rep
deleted / updated.

> Non-Repudiation

*: This provides the protection
the denial by one of the principals
involving in the comm.

- Availability

* Resource accessible / usable.

RFC 2828:-

* A Processing (or) comm service provided by a system to give a specific kind of protection to system resources.

Security Mechanism:-

* Feature designed to detect, prevent (or) recover from a security attack.

* no single mechanism that will support all services required.

* however one particular element underlies many of the security mechanisms in use. - cryptographic techniques.

X.800: > Specific Security mechanisms
> pervasive "

Specific Security mechanisms:-

* may be incorporated into the appropriate protocol layer in order to provide some of the OSI Security services.

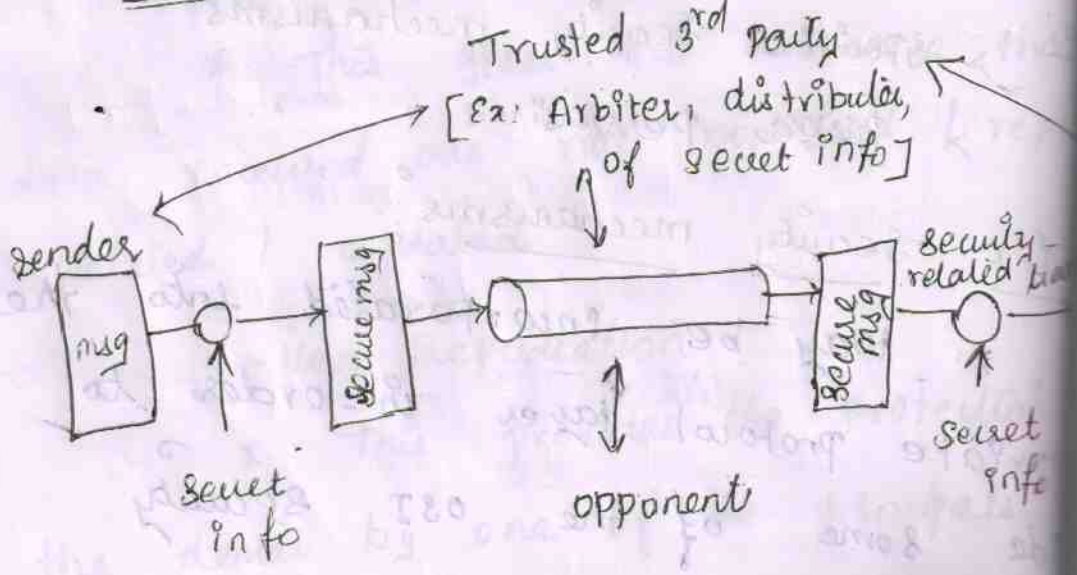
> Encipherment
> Digital signature
> Access ctrl
> Data Integrity
> Authentication
> Traffic pada
> Routing ctr
> Notarizat

* Pervasive Security Mechanism:-

*. Mechanisms that are not spe
to any particular OSI Security Servi
(or) protocol layer.

> Trusted functionality
> Security Label
> Event Detection
> Security Audit trail
> Security Recovery.

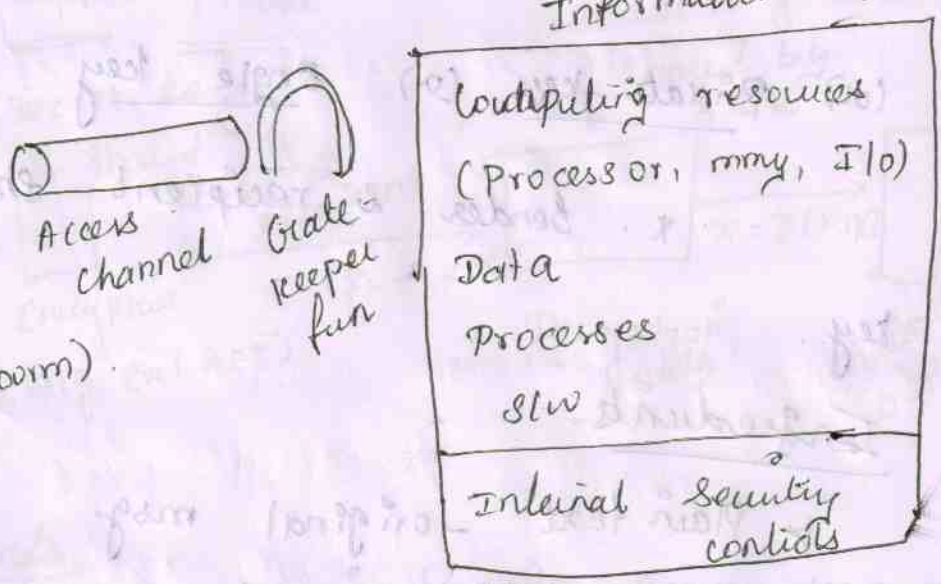
Network Security Model :-



Model for n/w security:-

* It requires us to the followings,
  - > Design a suitable algm for the security transformation.
  - > Generate the secret info (keys) used by the algm.
  - > Develop methods to distribute & share the secret info
  - > Specify a protocol enabling the principals to use the transformation & secret info for a security service.

Model for Network Access security :-



* Using network Access security model requires,
  - > Select appropriate gatekeeper fens to identify users.
  - > Implement security elets to ensure only authorised users access desig rated info (or) resources