

INTRODUCTION & NUMBER THEORY :-

- Introduction - (2)
- Services - (7)
- Mechanisms - (8)
- Attacks - (4)
- OSI Security architecture - (3)
- Network Security model - (9)
- classical Encryption techniques - (11)
 - > Symmetric cipher model - (11)
 - > Substitution techniques - (16)
 - > Transposition techniques - (25)
 - > Steganograph - (27)
- Finite fields and Number theory - (28)
 - Groups - (29)
 - Rings - (30)
 - Fields - (30)
 - Modular arithmetic - (31)
 - Euclid's algorithm - (33)
 - Finite fields - (34)
 - Polynomial Arithmetic - (35)
 - Prime numbers - (37)
 - Fermat's & Euler's theorem - (38)
 - Testing for primality - (40)
 - The Chinese remainder theorem - (40)

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 apps.

* Computer security:

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

* Information security:

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

* Computer Security :-

x. It is the collection of tools to protect data & thwart hacker is called computer security. (3)

* 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 In.

* OSI Security Architecture :-

x. OSI architecture provides a 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 (or) deliberate to evade security & violate the security policy of a system.

* Security Attack :-

(4)

* 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 net & 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 b/w the two principals.

* Active Attacks :-

* Involves alteration to the

Characteristics:-

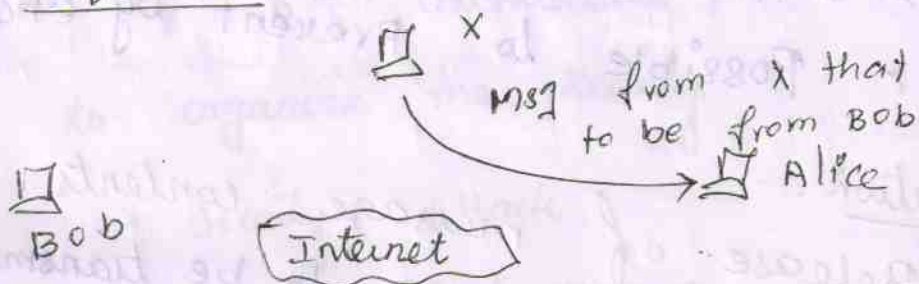
(5)

- > Difficult to prevent
- > Detection is feasible & can be recovered from the causes.

Classification:-

- > Masquerade
- > Replay
- > Modification of msgs
- > Denial of service
- > S/W attack.

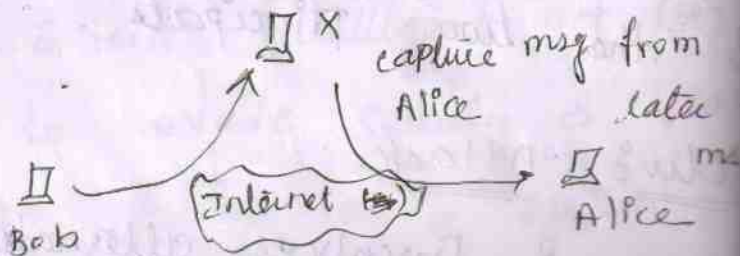
* Masquerade:-



* when one entity pretends to be a different entity.

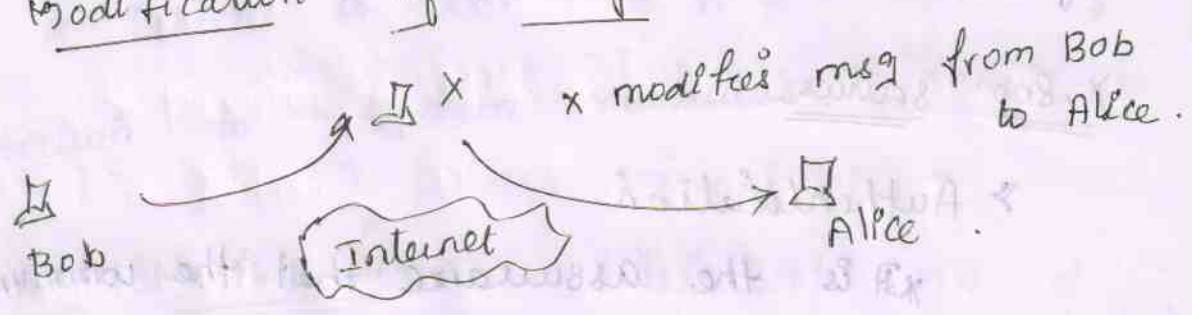
* the attacker captures the authentication & impersonates the sender.

* Replay:



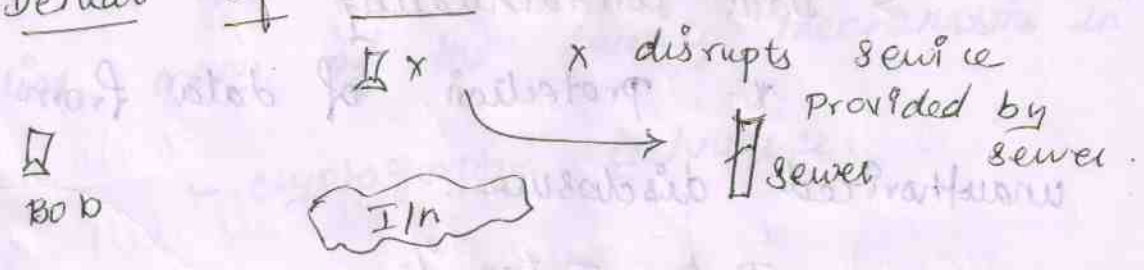
* The attacker captures the msg & retransmits the msg without any modification to (6) produce unauthorized effect.

* Modification of messages :-



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

* Denial of service :-



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

* Slow Attack :-

* Slow attacks are those which can be introduced into the systems (or) n/w. Ex: Worms, viruses.

Security Services - (4)

* Security service is a service provided by the protocol layer, which ensures security of the systems (or) data transfer.

Services :-

> Authentication

* It is the assurance that the communicating entity is the one that it claims to be.

> Access control

* The access control is the protection of a resource from unauthorized use of a resource.

> Data confidentiality

* Protection of data from unauthorized disclosure.

> Data Integrity

* This gives the assurance that data received are not modified / replicated / deleted / updated.

> Non-Repudiation

* This provides the protection against the denial by one of the principals involved in the communication.

- Availability

(8)

* 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.

> Encapsulation

> Authentication

> Digital signature

> Traffic padding

> Access ctrl

> Routing ctrl

> Data Integrity

> Notarization

* Pervasive Security Mechanism:-

* Mechanisms that are not specific

to any particular OSI Security Service

(or) protocol layer.

> Trusted functionality

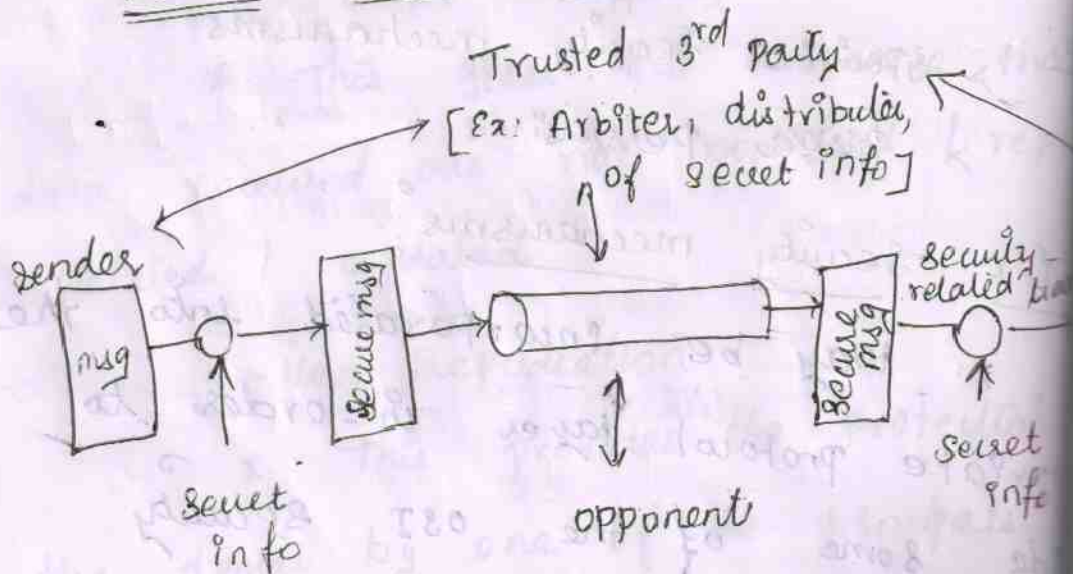
> Security label

> Event Detection

> Security Audit trail

> Security Recovery.

Network Security Model:-



Model for n/w security:-

(6)

It requires us to the following,

- > 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 :-

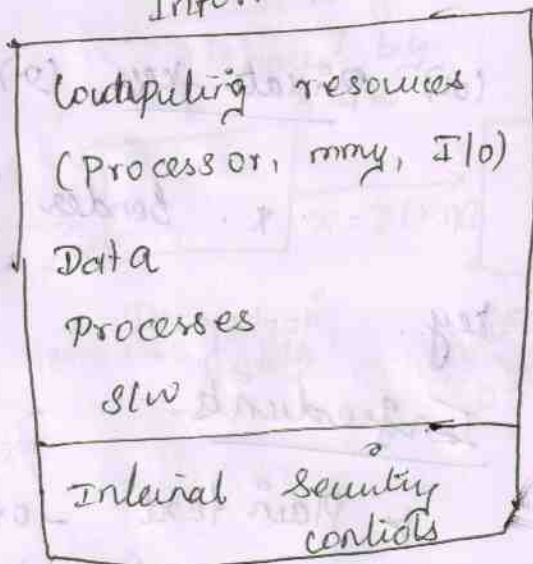
Information System

Opponent

- human (ex: hacker)
- slw (ex: virus, worm)

Access channel

Gatekeeper fun



Using network Access security model requires,

- > Select appropriate Gatekeeper funs to identify users.
- > Implement security clets to ensure only authorized users access designated info (or)

Information

Receiver

