UNIT-I

INTRODUCTION.

Security trends - Legal, ethical and Professional Aspects of security, Need for security at Multiple levels, security policies - Model of network security - Security attacks, services and mechanisms - OSI Security architecture - classical encryption techniques: substitution techniques, transposition techniques, Stegnography - Foundations of modern cryptography; perfect security - information theory - product cryptosystem - cryptanalysis.

Introduction :-

Security - Security is protecting the information from information risk.

Why security is important?

As security is ubiquotous. There is need for security due to the advent of electronic transactions and e-commerce process.

Solution :-

Here CNS (Cryptography) technique for the information security problems.

Cryptography - It is the process of storing and transferring data in a particular form. Hence only the intended persons can able to read and write.

This is the study and technique of building the ciphers to maintain and ensure confidentiality and integrity.

→ Information + Communication technique derived from mathematical model / calculation → algorithm, rules.

Information is considered as an Asset. Hence the Asset, information needs to be secured from any kind of attacks.

Three security goals: (CIA triad).

Confidentiality - protect the information from unauthorized third party access.

Integrity - protect the information from unauthorized change.

Availability - The information must be available to the authorized entity, whenever it is needed.

-> confidentiality is acheived by restricting the access
-> Integrity is acheived by restricting the data manipulation
-> Availability can be acheived by providing access to authorized person all time.

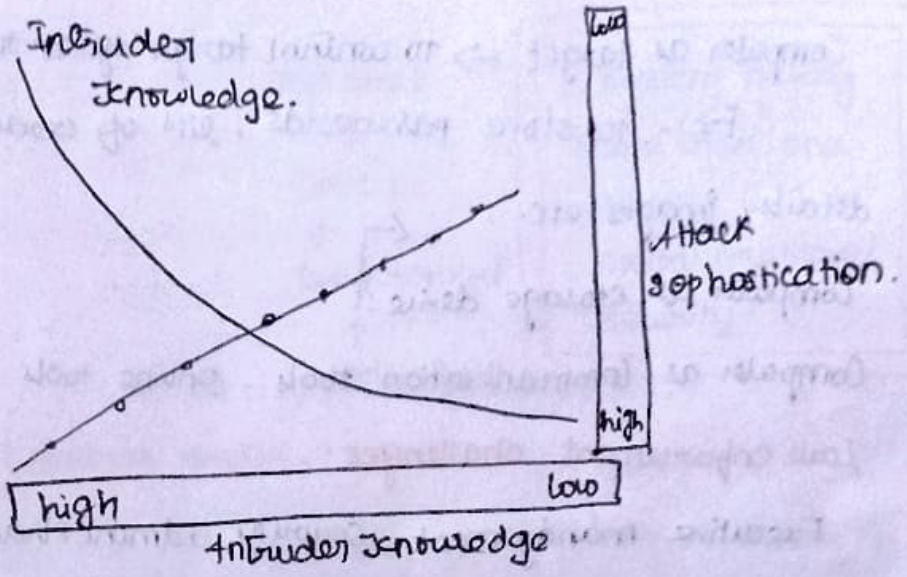
Examples:

Confidentiality - Concealment of information in military
Integrity - In Bank, account transaction has to be updated by authorized entities only.
Availability - Unavailability becomes harmful to the org.
Computer Security - Collection of tools designed to data collection and thwart hackers.

Network Security - measure to protect data during transmission.

Internet security - measures to protect data during transmission. ↓ This subject focus.

Security trends.



hence intruder knowledge at starting years and decreased in recent year due to stronger cryptographi-cal Techniques.

Legal, ethical and Professional aspects of security.

Cyber crime & computer crime

↓ involves computer Networks for criminal activities.

↓ involves computers for criminal activity, may or maynot Networks.

Here cryptography is used for secure transactions and to safe gaurd the personal Identifiable information.

→ To prevent tampering of document

→ To create trust between the servers.

Cryptography → invented by claude shannon. works at Bell lab.

↓ father of mathematical cryptography.

Scytale - earlier device of cryptography

Engima Enigma machine - Germany.

Modern cryptography uses Algorithms.

Computer crime :. Types.

Computer as target ⇒ to control target system to acquire info

Ex:- to store passwords, list of credit card details, images etc.

Computer as storage device :

Computer as communication tools - Online tools.

Law enforcement challenges :-

Executive management, security administrators have to check on law enforcement, tools, human factors etc...

↓ relies on technical and people skills.

→ org. should have proper criminal investigation process.

Intellectual property :.

↓

Intangiable assets, human ideas.

includes

↓

attacks ↓

→ Copyright → unauthorized use

→ Trade mark → unauthorized colorable & trademark

→ patents → unauthorized selling of patents

Infringement (attacks) on Ip attack.

DMCA → Digital millennium copyright.

This can be obtained when we store our own rights or content in digitialized manner.

DRM → Digital rights management.

ensuring the DMCA and checks for their work flow.

Privacy : Securing private information

↓

→ European union data protection directive

→ united states privacy initiatives.

→ organizational response