Cryptography & NW Security

Module - 1
Security Overview

Security - ensuring the (secrecy) confidentiality, data integrity & availability of components of computing system

CNS algorithms can be grouped into 4 main areas

① Symmetric → used to hide the contents of block or streams of data of any size, including messages, files, encryption keys & passwords

② Asymmetric encryption → used to hide small blocks of data, such as encryption keys, hash functions which are used in digital signatures

③ Digital integrity algorithm → used to protect blocks of data, such as messages from alteration

④ Authentication protocol - Schema based on the use of cryptographic algorithms designed to authenticate the identity of entities.

n/w Security - measure to protect data during their transmission

internet security → measures to protect data during their transmisson over a collection of interconnected n/w.

Computer security → The protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity & availability of information system resource(includes h/w, s/w, firmware, information /data & telecommunicat)

Confidentiality, integrity & availability are 3 levels of impact ~~from a security breach~~ keys of security

3 levels of impact from a security breach
- low
- moderate
- high (not taught by mabm)

Confidentiality

Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

privacy

making sure system is only accessible by authorized parties

Integrity

Assures that information & programs are changed only in a specified & authorized manner

- system integrity - assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- in simple terms system do it's job with out getting affected by unauthorized access

Availability

- Assures that systems work promptly and service is not denied to authorized users
- ensuring that authorized parties are not denied access to information & resources (accessing resources without only difficulty)

other goals

Non-repudiation - ensuring that communication parties can't later deny that exchange took place

Legitimate use - ensuring that resources are not used by unauthorized parties or in unauthorized ways

eg printer & disk quotas

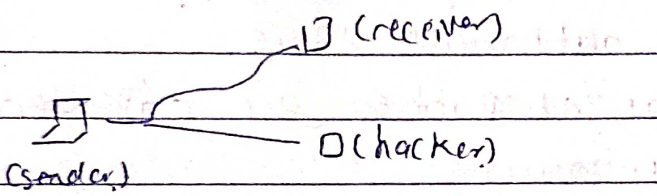
Spam filters in E-mail servers

Network S/w

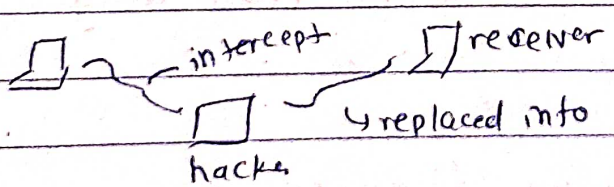
Four types of possibe attacks are

① Interruption : Services or data becomes unavailable, unusable, destroyed and so on such as lost of file, denial of Service etc

② interception : unauthorized subject has gained access to an object, such as Stealing data, overhearing others Communication



③ Modification : unauthorized Changing of data or tempering with services such as alteration of data, modification of message etc



④ Fabrication : additional data or activities are generated that would normally no exist. such as adding a password to a system, replaying previously send messages

OSI Security architecture

- ITU-T x 800 "Security architecture for OSI"
- defines a systematic way of defining and providing security requirements

3 aspects of information security
1. Security attack
2. Security mechanism
3. Security service

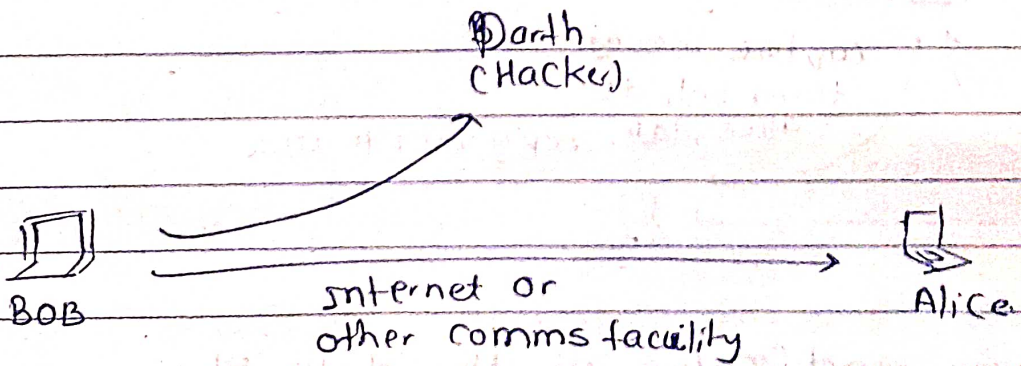
① Security attack

Any action that compromises the security of information owned by an organization

information security is about how to prevent attacks or failing that, to detect attacks on information based systems.

(i) passive attacks

a passive attack attempts to learn or make use of information from the system but does not affect system resources

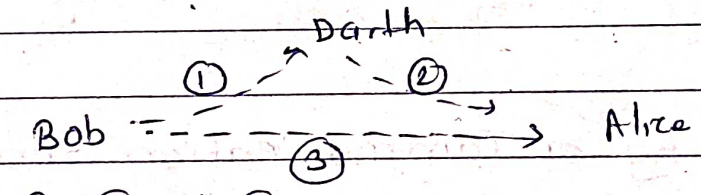


difficult to prevent because the wide vacity of potential physical, software, and n/w vulnerabilities

Goal is to detect attacks and to recover from disruption or delays caused by them

Masquerade → Takes place when one entity pretends to be diffrent entity
usually includes one of the other form of active attacks

Replay ⇒ involves the passive capture of data unit and its subsequent retransmission to produce an unauthorized effects



path ①, ② & ③

Modification of message → Some portion of a legitimate message is altered or message are delayed or reordered to produce an unauthorized effect
path 1, 2 active

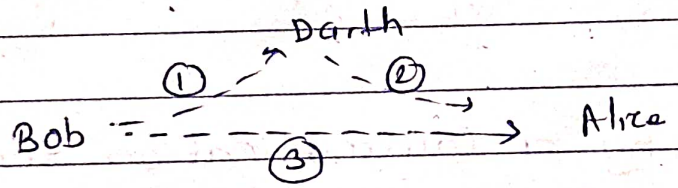
Denial of service → prevents or inhibits the normal use or managment of communication facilities (path 3 active)

difficult to prevent because the wide vacity of potential physical, software, and n/w vulnerabilities

Goal is to detect attacks and to recover from disruption or delays caused by them

Masquerade → Takes place when one entity pretends to be diffrent entity
usually includes one of the other form of active attacks

Replay ⇒ involves the passive capture of data unit and its subsequent retransmission to produce an unauthorized effects



path ①, ② & ③

Modification of message → Some portion of a legitimate message is altered or message are delayed or reordered to produce an unauthorized effect
path 1, 2 active

Denial of service → prevents or inhibits the normal use or managment of communication facilities (path 3 active)

② Security Service

- Enhance security of data processing systems and information transfer of an organization
- intended to counter security attacks
- using one or more security mechanism
- often replicates functions normally associated with physical documents

① X. 800:

a service provided by a protocol layer of communicating open system, which ensure adequate security of the systems or of data transfer

② RFC 4949

a processing or communication service provided by a system to give a specific kind of protection to system resource.

Security services (X. 800)

Authentication → assurance that the communicating entity is the one claimed

authentication service function ensure that two ends are authenticated, involes two parts.

① at the time of connection initiation, the service assures that the connection is the entity that it claims to be.

② service must assure that the connection is not integ interfered with in such that a third party can masquerade.

- peer to peer authentication - Provides for the corroboration of the identity of a peer entity is an association, two entities are considered peers if they implement to same protocal in different system.
eg two TCP modules in two communicating system

Data origin authentication - provides for the corroboration of the source of a data unit. does not provide protection against the duplication or modification of data units.
service supports application like email

Access Control - prevention of the unauthorized use of resource
it is the ability to limit and control the access to host systems & applications via communication links.
each entity trying to get access must be identified

Data Confidentiality - protection of data from unauthorized disclosure, passive attacks

Data integrity - assurance that data received is as sent by an authorized entity

Non-repudiation - protection against denial by one of the parties in a communication

⑤ Security Mechanism

- featured 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 mechanism in use
  - cryptographic techniques

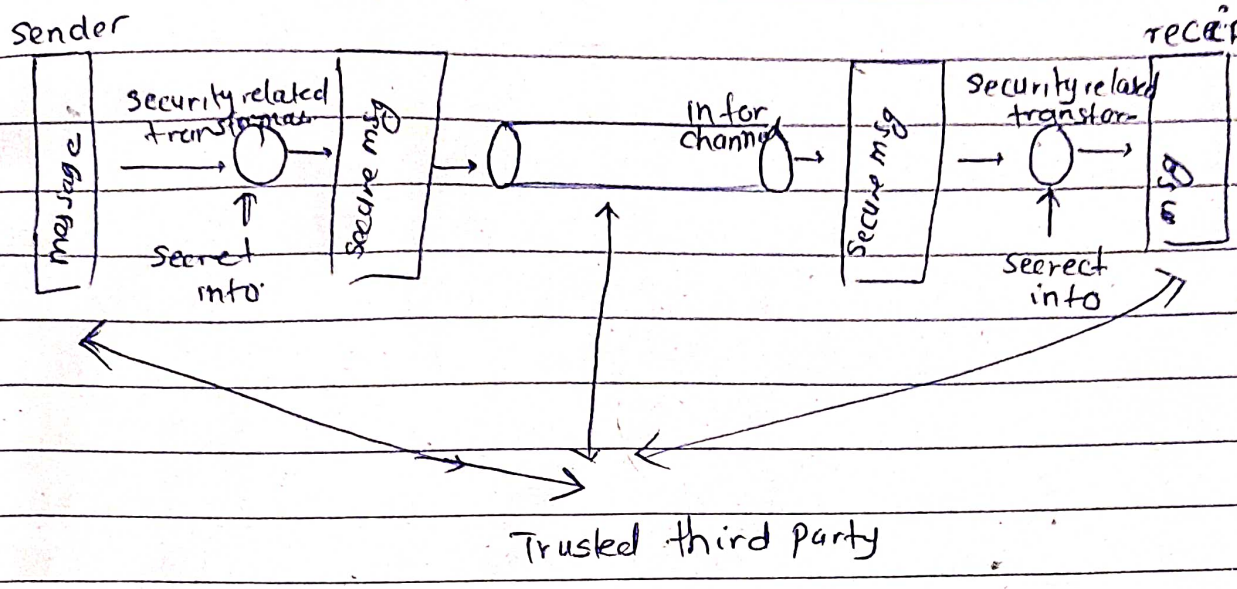
Specific Security Mechanisms

incorporated into the appropriate protocol layer inorder to provide some of the OSI security services

Encipherment → use of mathematical algorithms to transform data into a form that is not readily intelligible. the transformation and subsequent recovery of data depends on zero or more encryption keys.

Digital signature - Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit

- Model for network security



- a msg is to be transferred from one party to another across some sort of internet service. the two parties, who are principals in this transaction must cooperate for the exchange to take place
- logical information channel is established by defining a route through the internet from source to destination and by cooperative use of communication protocols (TCP/IP)
- Security related transformation on the mfo to be sent eg include encryption of the message which scrambles the message so that it is unreadable by the opponend & addition of a code based on the contents of the message can be used to verify identity of sender.
- Some secrect information shared by two principals and it is hoped, unknown to the opponent

using this model requires us to -

① design a suitable algorithm for the security transformation

② generate the secret information (key) used by algorithm

③ develop methods to distribute and share the secret information

④ specify a protocol enabling the principals to use the transformation & secret information for a security service

Classical Encryption Techniques

Basic Terminology

- Plaintext - original message
- Ciphertext - coded message
- Cipher - algorithm for transforming plaintext to Cipher text
- key - info used in cipher known only to sender/receiver

Encipher (encrypt) - converting plaintext to ciphertext

Decipher (decrypt) - recovering ciphertext from plaintext

cryptography - study of encryption principles / methods

Cryptanalysis (codebreaking) - Study of principles / methods of deciphering ciphertext without knowing key

Cryptography - field of both cryptography & Cryptanalysis

Classical Substitution Ciphers

letters of plaintext are replaced by other letters or by numbers or symbols

if plaintext is viewed as a sequence of bits then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

① Caesar Cipher

earlist known substitution cipher

replace each letter by 3rd letter

eg

meet me after

PHHW PH DIWU

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

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

Cryptanalysis →

- only have 26 possible ciphers
- simply try each turn
- brute force search
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext

② Monoalphabetic Cipher
- rather than just shifting the alphabet
- shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to different random cipher text
- hence key is 26 letters long

Plain : abcdefghijklmnop...
Ciphe.: DKVQFIBJW....

now have total 26! ⇒ 4x1026 keys

Cryptoanalysis
e is most used alphabet in english followed by T, R, N, I, O, A, S
in Monoalphabetic cipher relative frequency of alphabets doesnot change
by Counting frequency in Cipher text it can be mapped with mostly occuring free alphabet relatively
with this method message can be decoded.

③ Playfair Cipher
- not even the large no. of keys in a monoalphdbetic cipher provides security
- one approach to improving security was to encrypt multiple letters

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

→ 5x5 matrix of letters based on a keywards
→ matrix based on keyword MONARCHY fill remaining letters randomly

Encrypting & Decrypting

plaintext is encrypted two letters at a time
→ if pair is repeated letter, insert filler like 'x'
- if both letters fall in the same row, replace each with letter to right (wrapping back to start to end)
→ if both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom)
→ otherwise each letter is replaced by the letter in the same row and in column of the other letter of the pair.

Security:
→ much improved over monoalphabetic
→ 26 x 26 → 676 diagrams
- need 676 entry frequency table to analyse & corresponding more ciphertext.

④ Polyalphabetic Cipher
- improve security using multiple cipher alphabets
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message.
- use each alphabet in turn
- repeat from start after end of key is reached

⑤ Vigenere Cipher

- simplest polyalphabetic substitution cipher
- effectively multiple caesar cipher
- key is multiple letters long $K = k_1 k_2 \ldots k_d$
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse

$C = E(k, p) = (p + k_i) \bmod 26$

key → deceptive

key → deceptive deceptive deceptive
wearediscoveredsave yourself

ciphertext → ZICVTWQ ....

$(d + w) \bmod 26 \Rightarrow Z$

$(e + e) \bmod 26 \Rightarrow I$

Security of vigenere ciphers ⇒

- have multiple ciphertext letters for each plaintext letter
- hence letter frequencies are obscured but not really lost
- start with letter frequencies
  See if monoalphabetic cipher or not
- if not then need to determine no. of alphabets, since then can attack each

⑥ Autokey Cipher

→ ideally want a key as long as message
→ Vigenere proposed the autokey cipher with keyword is prefixed to message as key
→ knowing keyword can recover the first few letters use these in turn on the rest of the message

- but still have frequency characteristics to attack

key : deceptiveweareDiscovedSave
weareDiscoveredSaveyourself

Cipher

$$C_i = (K_i + P_i) \bmod (26)$$

One Time Pad

- Truly random key as long as the message is used, the cipher will be secure
- Called one-Time Pad
- unbrakable since Ciphertext bears no statistical relationship to the plaintext
- security of the one time pad is entirely due to the randomness of the key.
- If the Stream of character that constitute the key is truely random then the stream of characters that constitute the cipher will be truly random.

Transposition Ciphers

- These hide the message by rearranging the letter order
- without altering the actual letters used
- Can recognise these since have the same frequency distribution as the original text

Rail Fence Cipher

- write message letters out diagonally over a no of rows
- then read off cipher row by row
- eg. meet me after the toga party

m e m a t r h t g - - - -
e t e t e t e o a - - - -

memathrhtgetetetoa

Row Transposition Ciphers

- more complex transposition
- write letters of messages out in rows over a specified no. of columns
- then reorder the columns according to some key before reading off the rows

Keys: 4 3 1 2 5 6 7

a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

Cipher TTNAAPTMTSUOAODWL

while converting cipher (2 1 4 3 6 5 7) these column order followed

ROTOR Machine

⇒ before modern ciphers, rotor machine were most common complex ciphers in use
→ widely used in WW2
→ implemented a very complex, varying substitution cipher
→ used a series of cylinders, each giving one substitution cipher, which rotated and changed after each letter was encrypted
→ with 3 cylinders have $26^3 \Rightarrow 17576$ alphabets
→ machine consists of a set of independently rotating cylinders through which electrical pulses can flow
→ each cylinder has 26 i/p pins & 26 o/p pins with internal wiring that connects each input pin to unique o/p pin

Steganography

⇒ Alternative to encryption
→ hides existence of message.
- using only a subset of letters/words in a longer message marked in some way

→ Simple form of steganography, but one that is time consuming to construct, is one in which an arrangment of words or letters within an apparently text spells out the real message.

Character marking - selected letters of printed or typewritten text are over-written in pencil. the marks are ordinarily not visible unless the paper is held at an angle to bright lines

Invisible Ink - a no. of substances can be used for writing but leave no visible trace untill heat or some chemical is applied to the paper

pin punctures: Small pin punctures on selected letters are ordinarily not visible unless paper is held in front of a light

Typewriter correction ribbon: used blw lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Security information theoretic aspect

Steganographic algorithm to be r secure if the steganographic relative entropy blw the cover object & stego. objects pdf is very small

- false alarm prob.
- Detection prob.
- if $P_{FA} = P_{det}$ then detector makes purely random guess

∴ the steganography algo is r secure ($0 < \gamma < 1$) if $|P_{FA} - P_{det}| \leq \gamma$.

Steganography vs Cryptography

parameter	steganography	cryptography
Integrity	structure of data remains same	can be altered
Security principles	supports confidentiality & authentication	additionally supports non repudiation & data integrity
Recovery of original data	loss of carrier signal	one to one function no loss of plain text
Altering Capacity	partly altered below threshold	Entire plaintext get altered
Content adaptive change	more hiding in dense content	uniform change
Trap door function	Estimation methods, no keys	requires keys.

Steganography	Cryptography
Conceals the existence of msg	Hiding the contents of a secret message from malicious people
does not alter the structure of secreat msg but hides it inside a cover file so it cannot be seen.	Cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is provided
makes secret msg unseen	encrypt the message but it can be seen.

Types of Steganography

Image → using least significant bit (LSB) method by replacing least bits with the msg to be encoded.

Text → n^{th} letter of every word

audio → Same as image

LSB → last bit is changed with hiding content

Hiding a trademarks or identification for the use of determining ownership

watermarking

public/blind	private/non-blind
original signal is not required during detection	original signal is required during detection

Divisibility & division algorithm.

a|1 then $a = \pm 1$

$a|b, b|a \Rightarrow a = \pm b$

Euclidean algorithm

- Simple procedure for determing the greatest common divisor of two +ve integers.
- two integers are relatively prime if and only if their only common positive integer factor is 1