Operating System & Computer Security

2016

(01) i) Computer security : protection of the items you value - assets of the computer or computer system.

ii) Security Service | Security mechanism

ex: Encryption.

x800 : a service provided by a protocol layer of communicating open system, which ensures adequate security of the systems or of data transfers.

RFC 2828 :- a processing or communication service provided by system to give a specific kind of protection to system resources.

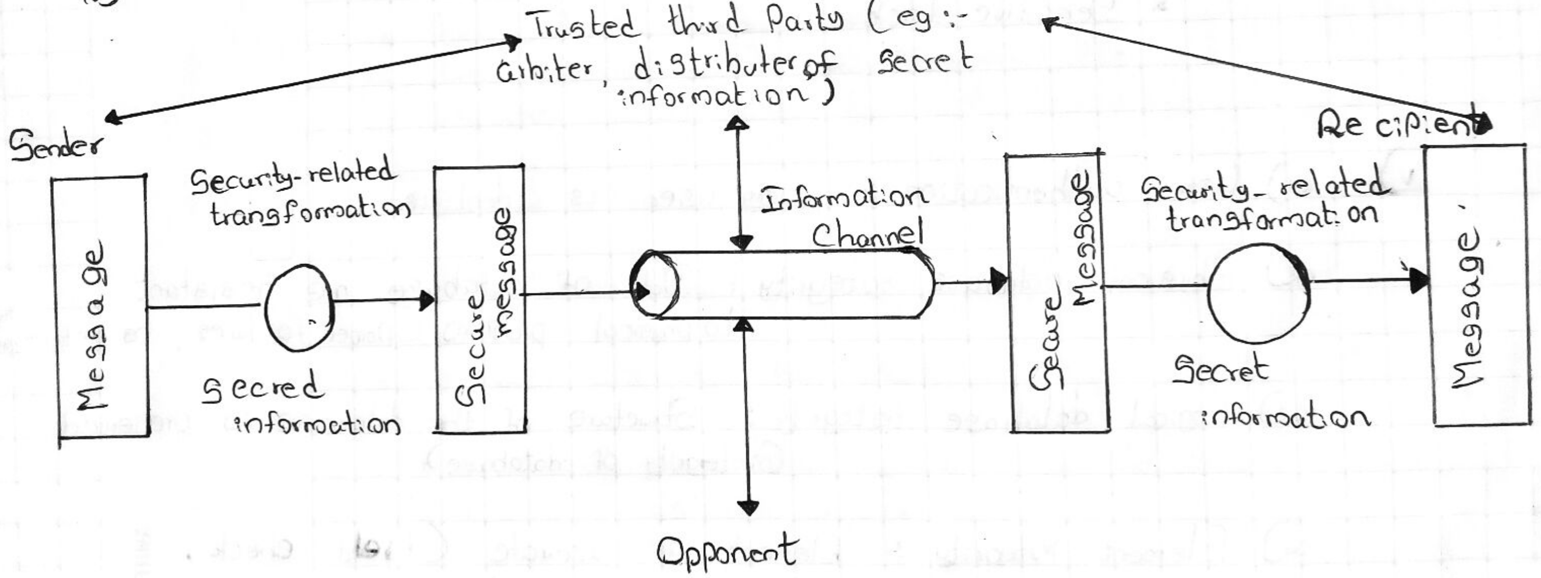
* a machanism that is designed to detect, prevent or recover from a security attack.

iii) Security attack :- any action that compromises the security of information owned by an organization.

Passive attack :- eavesdropping on. or monitoring of transmission to : ...

active attak : modification of data stream to : ...

iv)



Trusted third Party (eg :- arbiter, distributer of secret information)
Sender
Recipient
Security-related transformation
Message
Secure message
Secred information
Information Channel
Secure Message
Security- related transformation
Secret information
Message
Opponent

v) a) Interception :- unauthorized party has gained access to an asset
(මැදිහත්විම)

b) Modification :- unauthorized party
(Data Edit)

c) Interruption. :-
(බාධාවෙන)

(Password & Access control)

② i) Server
Server Encrypt
Client

ii)
- * Establishing data definition
- * Developing programs to generate needed information.
- * Adding data & deleting data from the database.
- * Implementing Security & integrity controls.
- * Managing database operations
- * Database planning and Development.

iii)
- * It should be at least 6-8 characters long and Should Include at least two uppercase letters, lowercase letters and numbers
- * Password may not contain your username or any part of your full name.
- * Passwords must contain characters from at least threee of the four class characteristics.
- * It should be easy for you to remember.

iv)
- * Integrity lock
- * Sensitive lock

v)
01) User authentication :- every user is identified

02) Physical database integrity :- Data of database are resistant to physical problem. (Power failures, os protection)

03) Logical database integrity : Structure of the database is preserved. (integrity of database).

04) Element integrity :- Element are accurate (field check, Access control, chang log)

05) Access control :- Logically separated for users. Allowed to access only authorized data.

(03)

i) 01) decrypt :- Recovering plaintext from ciper text

02) cipher text :- The coded message.

03) Cryptology :- The field of both cryptography and cryptanalysis.

04) key :- Information used in cipher known only to sender/receiver

05) Encrypt :- Converting plain text to cipher text.

06) Cryptography :- Study of encryption principles / methods

07) Plain text :- The original message.

08) Cryptanalysis :- The study of principles / methods of deciphering cipher text without knowing key.

09) Cipher :- Algorithms for transforming plaintext to cipher text

ii)
- * type of encryption operations used.
- * number of keys used.
- * way in which plaintext is processed.

iii) a) Caease Cipher

- * by Julius Caesar
- * first attested use in military affairs.
- * replace each letter by 3rd letter on.

b) Simple Columnar transposition technique -

key type
way of Plain text
Encryption Operation,

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

iv)
```
# include <iostream.h>
# include <conio.h>
void main
   {
     clrscr();
     Char plaintext [26] = "ABCD..     z " ;
     int key = 3 ;
     Cout << " Enter plain text:" ;
     Cin >> plaintext >> endl ;
     Cout << "Cipher text :   " ;
        for ( int i=0 ; i<= size of (Plaintext) - 1 , i++)
        { cout << char (( 65 + ( int (Plaintext [i]) - 65 + key  ) % 26 ));
     getch ();
   }
```

Q4 i) a) Digital Signature :- • have looked at message authentication.
- but does not address issues of lack of

• digital signatures provide the ability to
- Verify author, date & time of signature.
- authenticate message content.

b)

Digital Certificate :- An electronic document which provides the certification that a person is ~~authentication~~ authorised to use the public key Algorithm given to him by a trusted third party

ii)

Digital Signature	Manual Signature
* A digital signature is a mathematical scheme for presenting the authenticity of digital message or document. * the sender cannot deny having sent the message. * the message was not altered in transit (integrity)	* A signature is a handwritten depiction of some one's name

iii)

Digital Signature
Key Encryption
Object Signing

iv)

Version
Subjects
Issuers
Validity peorod
Public key
Algorithms used
Certificate extensions.

v)

vi)

(05) i) Any software that harms to a Computer System

ii) Get Slower than your machine.
Created copies itselfs
always restarting your machine.

iii) Trapdoor :- * Secret entry point into a program
* allows those who know access bypassing usual Security procedures

iv) * Packet filters
* Stateful packet filter
* Application level Gateway
* Circuit Level Gateway.

v)

Packet filtering	application level firewalls.
* Simplest, fastest firewall component	* have application specific gateway
* foundation of any firewall system.	* has full access to protocol
* Possible default policies	* need separate proxies for each Service.

vi) a) Password Guessing :- * One of the most common attack
* attacker knows a login. (from email / web page etc)
* Check by login or against stolen password file.
* Success depends on password chosen by user

b) password Capture. :- * another attack involves password capture.
* Using valid login / password can impersonate user.
* users need to be educated to use suitable precautions

d) approaches to Intrusion Detection.

- Statical anomaly detection
  - threshold
  - profile based

- Rule-based detection
  - anomaly
  - penetration identification.