UNIT IV

SECURITY PRACTICE & SYSTEM SECURITY

UNIT - IV

(2)

Security Practice & System Security.

Authentication Applications :-

* key concern of security are confidentiality and timeliness.

* To provide confidentiality one must encrypt identification field & session key.

* Developed to support application - level authentication and digital services.

* kerberos - a private key authentication sewice.

* X.509 - a public key directory authentication sewice.

kerberos :-

* kerberos is a centralized authentication sewer, whose fun is to authenticate the users to sewer and sewer to users.

Problem that kerberos address in this :-

Workstation cannot be trusted to identify its users correctly to nlw,

threats, > masquarade
> Eavesdropping
> Replay.

Requirements of kerberos :-

- Secure
- Transparent
- Reliable
- Scalable.

kerberos version 4 :-

* This make use of DES.

* Simple Authentication Dialogue :-

* To overcome unauthorized users to access, it means to use an authentication sever (AS) that stores password of all users and shows a unique secret key with each sever.

(1) $C \rightarrow AS : IP_C \,||\, P_C \,||\, ID_V$

(2) $AS \rightarrow C$: Ticket

(3) $C \rightarrow V : ID_C \,||$ Ticket

$$\text{Ticket} = E(k_V, [ID_C \,||\, AD_C \,||\, AD_V])$$

Steps:

* Users logs on to a workstation & request access to sever.

* Ticket is encypted, so it is not altered by C (or) opponent.

* The ticket is decypted by V and verify the user ID.

Adv:

* As ticket is encrypted, it prevents alteration by C. (4)
* Inclusion of ADc in the ticket, avoids attack by an opponent.

Disadv:

* Each ticket can be used only once
* Pwd is used as clear plain text Pc, opponent can misuse it.

* More Secure Authentication Dialogue:-

* this provided by use of ticket granting Sever (TGS) instead of authentication Sever (AS).

Scenario:-

once per user logon section:

(1) C → As : IDc || IDtgs

1. tgs authenticate client & provide ticket

(2) AS → C : E(Kc, Ticket tgs)

2. ticket encrypted with session key, client will decrypt it

once per type of severice:

(3) C → TGS : IDc || IDv || Ticket tgs

(4) TGS → C : Ticket v.

Once per Sevice Session:

(5) C → V : ID_C || Ticket V.

Encrypted ticket shared by sever & TGS.

Ticket contains following information:

$Ticket_V = E(K_V, [ID_C || AD_C || ID_V || TS_2 || Lifetime_2])$.

$Ticket_{tgs} = E(K_{tgs}, [ID_C || AD_C || ID_{tgs} || TS_1 || Lifetime_1])$.

Adv:-

* Ticket reusability.
* Protection of user password.
* Timestamps indication of issuing tickets date and time.
* Encryption tgs and tv prevents forgery.

* V4 Authentication Dialogue:-

* Combination of simples & more secured authentication.

V4 Message Exchanges:-

a) Authentication sever exchange to obtain ticket-granting ticket.

(1) C → AS : $ID_C || ID_{tgs} || TS_1$

(2) AS → C : E(Kc, [Kc, tgs || IDtgs || TS2 || Lifetime 2 || Ticket tgs]) (6)

3) Ticket - Granting sewice exchange to obtain sewice - granting ticket.

(3) C → TGS : IDv || Ticket tgs || Authenticator C

4) TGS → C : E(Kc, tgs, [Kc,v || IDv || TS4 || Ticket v])

Ticket tgs = E (Ktgs, [K C, tgs [K C, tgs || IDc || ADc || IDtgs || TS2 || Lifetime 2) .

Ticket v = E (Kv, [Kc,v || IDc || AD c || IDv || TS4 || Lifetime 4])

Authenticator c = E (Kc, tgs, [IDc || ADc || TS3]) .

5) Client / sewer authenticate exchange to obtain sewer:

(5) C → V : Ticket v || Authenticator c.

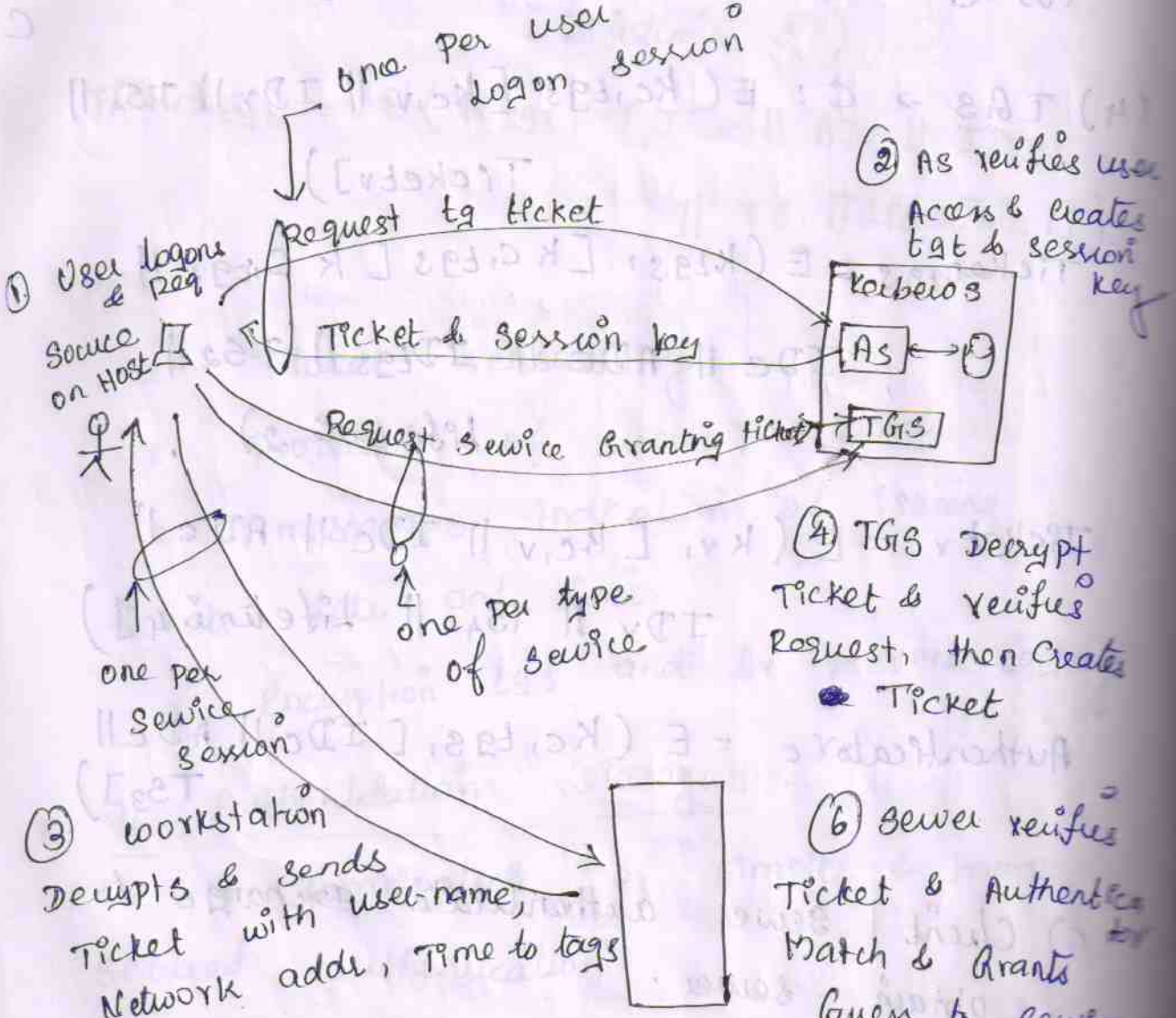
(6) V → C : E (Kc,v, [TS5 + 1)

(for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_c \| AD_c \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,v}, [ID_c \| AD_c \| TS_5])$

Overview of kerberos:-



(5) Workstation sends Ticket and authenticator to server.

Kerberos Version 5:-

(*) Encryption System dependence

* Internet protocol "

* Msg byte ordering

* Ticket lifetime

* Authetication Forwarding in V5 not in V4.

* Inter-realm authentication.

V5 Message Exchanges:-

a) Authentication souxe exchange to obtain tags:

(1) C → AS: Options || IDc || Realm c ||
IDtgs || Times || Nonce1

(2) AS → C: Realmc || IDc || Ticket tgs ||
E(Kc, [Kc, [Kc, tgs || Times || Nonce1 ||
Realm tgs || IDtgs]).

Ticket tgs = E(Ktgs, [Flags || Kc, tgs ||
Realm c || IDc || ADc || Times])

b) Ticket-granting source Exchange to obtain source-granting ticket:-

(3) C → TGS: Options || IDv || Times ||
Nonce2 || Ticket tgs || Authenticator C.

(4) TGS → C : $Realm_C \| ID_C \| Ticket_v \|$

$E(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \|$

$Realm_v \| ID_v])$

$Ticket_{tgs} = E(K_{tgs}, [flags \| K_{c,tgs} \| Realm_c$

$\| ID_c \| AD_c \| times])$

$Ticket_v = E(K_v, [flags \| K_{c,v} \| Realm_c \|$

$ID_c \| AD_c \| Times])$

$Authenticator_C = E(K_{c,tgs}(ID_c \|$

$Realm_C \| TS_1])$

C) Client / Server Authenticate exchange to obtain service :-

(5) C → V : Options $\|$ Ticket$_v$ $\|$ authenticator

(6) V → C : $E_{K_{c,v}}[TS_2 \| subkey \| seq\ \#]$

$Ticket_v = E(K_v, [flags \| K_{c,v} \| Realm_c$

$ID_c \| AD_c \| Times])$

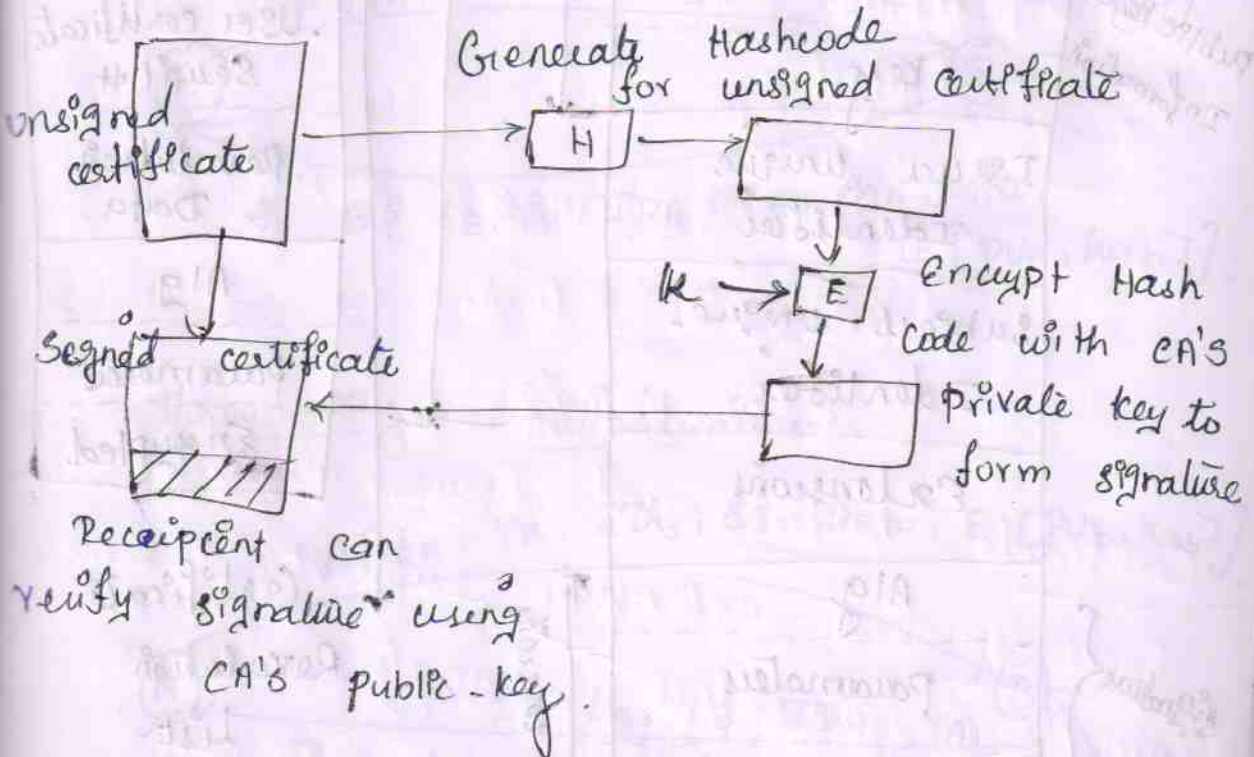
$Authenticator_C = E(K_{c,v}[ID_c \| Realm_c \|$

$TS_2 \| subkey \| seq\ \#])$

X.509 Authentication Service :- (10)

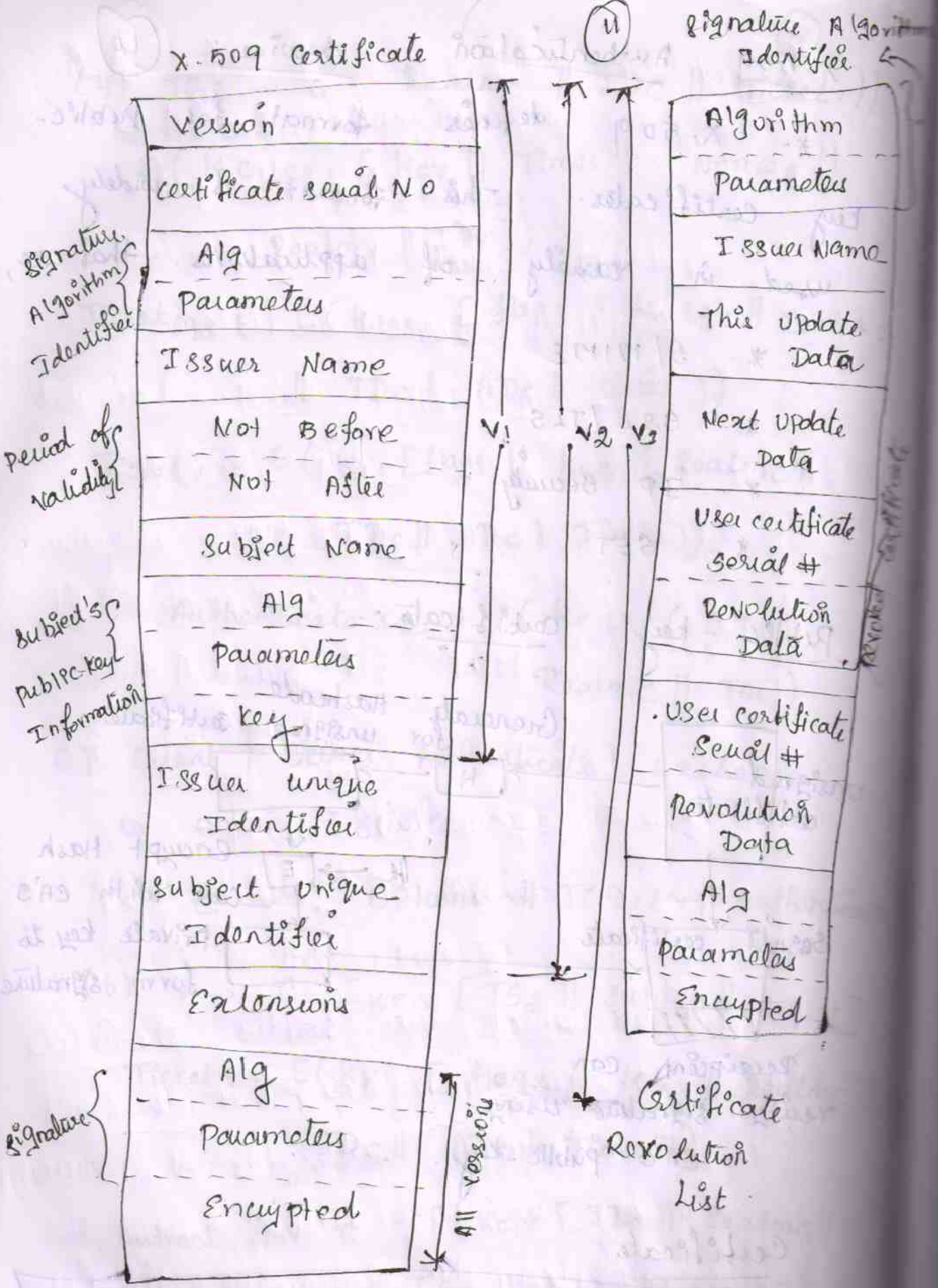
* X.509 defines format for Public-key certificates. This format is widely used in variety of applications. that are,
  * S/MIME
  * SSL/TLS
  * IP Security
  * SET.

Public-key certificate :-



Certificate

$$CA\langle\langle A\rangle\rangle = CA\{V, SN, AI, CA, TA, A, Ap\}$$

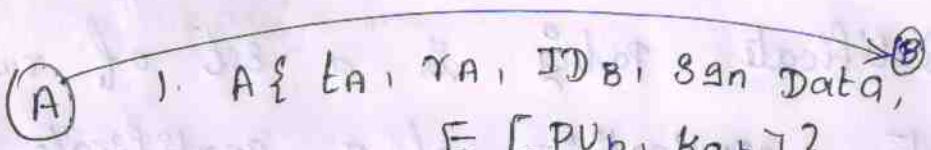


Two types of certificates:-

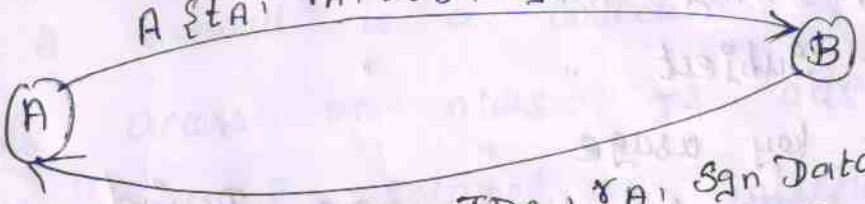
* Forward certificates
* Revesse " .

Authentication procedures:-

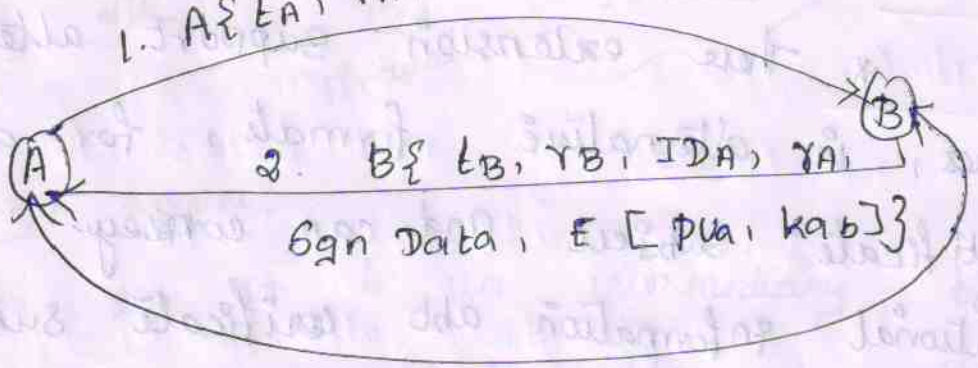
* One-way Authentication:-



* Two-way Authentication:-



* Three-way Authentication:-



X.509 Version 3:- (13)

Certificate extensions fall into 3 main categories

> key and policy info
> subject and Issue attributes
> Certification path constraints.

key and Policy information :-

Certificate policy is a set of rules that indicates applicability of a certificate to a particular community. It includes,

> Authority key identifier
> Subject " "
> key usage
> private key usage Period
> certificate policies
> Policy mapping.

Certificate subject and Issue attributes :-

* These extension support alternative names, in alternative formats, for a certificate subject and can convey additional information abt certificate subject.

> Subject alternative name
> Issuer " "
> subject directory attributes.

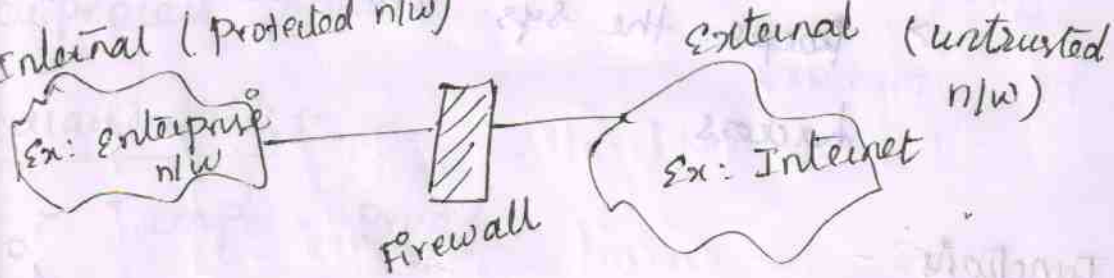
Certificate Path constraints:-

* Allow constraint specifications to be included in certificates issued for CA's by other CA's.

> Basic constraints
> name "
> Policy "

Internet Firewalls for Trusted System:-

* A firewall is a collection of devices controls access on n/ws. It acts as a filtering wall for internet & internet to ensure security.



Proxy sever:-

* It is an intermediary b/w a web-browser & the I/n. It helps to improve web performance by storing a copy of frequently used web-pages

Role of Firewalls: —

* The primary role of firewall is to protect computer n/w from threats.

* A firewall acts an efficient protecting tool for the system. This is a security pgm which protects n/w from unauthorized access (or) corruption. It can automatically reject and decrypt the unwanted 'info' through the n/w.

Benefits:-

> Less expensive
> detect viruses, worms & trojans.
> keeps the sys well secured from hackers.

Functions:-

* Creates a n/w address & hides private address.
* Reduces the vulnerability of sys
* Breaks the info to small pcks to enable easy scanning.
* Serves as a guard for more than one computer.

Firewalls are implemented to,

* Ensure security of n/w.
* claim trust on each entity participant in a n/w.
* To simplify the security policy to be developed on each individual components in a n/w.
* To provide global security platform to a n/w.

Design of Firewalls :-

* A firewall acts as a reference monitor. Reference monitor is a collection of access controls for files, memory, devices, interprocess comm ....

Characteristics :-

> Tamper - Proof
> Un by passable
> Analyzable.

Firewalls can be designed as,

> Packet filtering gateway / Screening routers
> guards.

> Stateful inspection firewalls
> appln proxies
> Personal firewalls.

Firewall Related Terminologies :—

* Firewall is a device that enforces an access ctl policy amg n/ws.
  > Protected n/w
  > Unprotected n/w
  > Demilitarized zone (DMZ)
  > Dual - Homed firewall
  > Tri - Homed "

* Proxy stands b/w the protected & un-protected n/w. There are 2 types of proxies,
  > Application proxies
  > Circuit proxies.
  > policy
  > Authentication
  > Security association
  > Packet filtering
  > stateful "
  > Logging.

Limitations of Firewall :-

* Cannot protect from attacks by - Paring it
* cannot protect against Internal threats
* cannot protect against access via WLAN
* cannot protect against malware imported.

SET for E-Commerce Transactions :-

* Secure Electronics Transaction (SET) a comm protocol std developed to secure credit card transactions on unsecure nws, the Internet.
* SET enables participants to exchange info securely.

Key Features :-

* Info confidentiality.
* Data Integrity
* Card holder
* Merchant
* Issuer
* Certification Authority.

SET on E-Commerce:-

* The customer opens a Mastercard account. The customer receives a digital certificate. It includes a public key of merchants and bank's.

E-commerce transactions:-

* The dual signature is to link
  > OI (order information)
  > PI (payment ")

* The MD - message digest of the OI & the PI are independently calculated by the customer.

INTRUDERS:-

* Unauthorized person accessing the info from computer system (or) n/w is called intruders / hackers / crackers.

Three classes of Intruders:-

* Masquerader (Insider)
* Misfeasor (Outsider)
* Clandestine User (either Insider (or) outsider)

Intrusion Techniques:-

> Gain access to the system
> To increase the range of privileges accessible on a system.

Password file protected in 2 ways:-

(1). One-way Function:-

* the sys stores only value of fun based on user's pwd. when user types a pwd, the sys transforms pwds & compare it with stored value.

(ii) Access ctrl:-

* Access to the pwd file is limited to one (or) a very few accounts.

* the pwd crackers, report following techniques for learning pwds,

> Try default passwords.
> Try all short "
> Try user's phone number, SSN, room No.
> Use a Trojan horse.
> Tap the line b/w remote user and host system.

Intrusion Detection

* If intrusion detected quickly, the intruder can be identified & ejected from sys before any damage is done.

* An effective intrusion detection sy can serve as deterrent, so to prevent intrusion.

* Intrusion detection can be used to strengthen intrusion prevention facility.

* counter measures for intrusion are,
  > Detection
  > Prevention.

Approaches:-

a) Statistical Anamoly Detection:-

* Involves collection data relating to the behaviour of user over a period time.
  > Threshold Detection
  > Profile based.

b) Rule based Detection:-

* Defines a set of rules that can be used to decide that a given behaviour is that of an intruder.

> Anamoly Detections

> Penetration identification.

Audit Records (AR):-

* AR is a tool for intrusion detection.

> Naive Audit Records:-

* Virtually all multi-user OS include accounting s/w that collects info on user activity.

Adv: Extra s/w is not needed.

Dis-adv: Has no proper format of info.

> Detection-Specific Audit Records:

* A collection facility can be implemented that generates AR containing info needed by intrusion detection sys.

Adv: Vendor independent

Dis-adv: Extra overhead due to running two packages in same machine.

* It contains, subject, Action, Obj, Exception condition, Resource usage, Timestamp

IDES Approach:-

* Based on examination of audit record
* Entries are matched against rule base to detect intrusion.

Draw backs:-

> Lack of flexibility
> Difficult to point-out slight variation in explicit rules.

Viruses and Related Threats:-

* Perhaps the most sophisticated types of threats to computer systems are presented by pgms that exploit vulnerabilities in computing systems.

Malicious Pgms:-

* Virus
* Worm
* Logic bomb
* Trojan horse
* Backdoor - (trapdoor)
* Zombie
* Keyloggers
* Root kit

The nature of viruses :-

* A virus is piece of slw that can "infect" other pgms by modifying them; the modification includes a copy of the virus pgm, which can then go on to infect other pgms.

4 - Phases :-

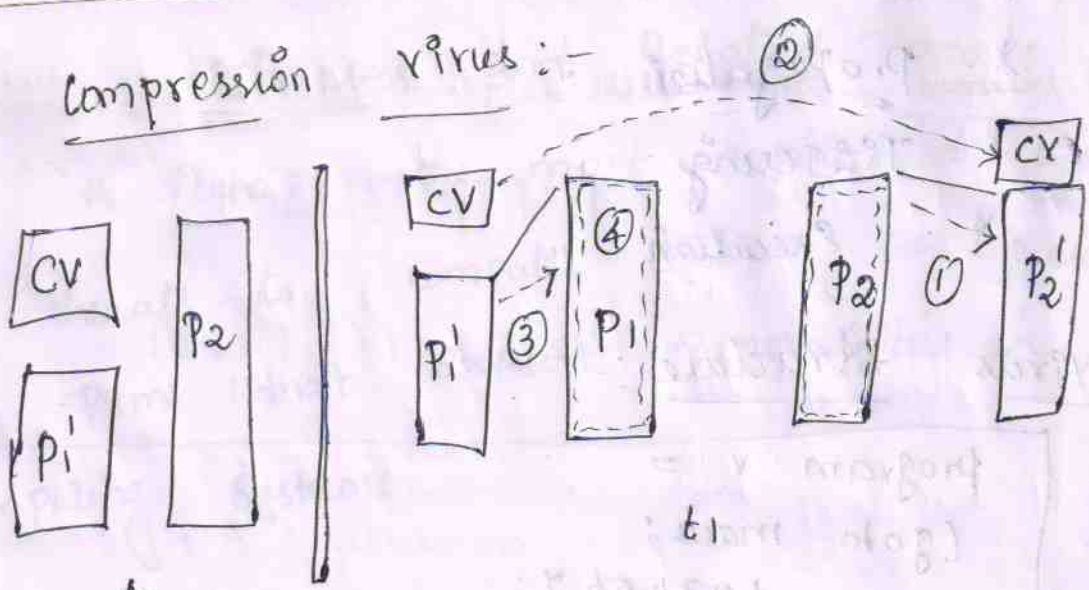
* Dormant Phase
* Propagation "
* Tiggering "
* Execution "

virus structure :-

```
program V :=
{goto main;
      1234567;
   subroutine infect-executable :=
   { loop:
        file := get random-executable-file
     if (first-line-of-file =
                1234567
     then goto loop
        else prepend V to file;}
   Subroutine do-damage :=
        {whatever damage is to be done}
```

```
Subroutine trigger_pulled :=
        {return true if some condition
                                holds}
main:   main_program :=
                { infect_executable;
                  If trigger_pulled then
                                do_damage;
                  Goto next;}
        } next :
```

Compression virus :-



Types of virus :-

* Parasitic virus
* Memory-resident "
* Boot-sector "
* Stealth "
* polymorphic "
* metamorphic "

E-mail viruses:-

* The E-mail virus sends itself to everyone on the mailing list in the user's e-mail Package.

* The virus does local damage.

Worms:-

* A worm is a pgm that can replicate itself and send copies from computer to computer across n/w connections.

Ex: * electronic mail facility

* Remote execution capability

* Remote login "

State of worm technology:-

* Multi-Platform
* Multi-exploit
* Ultra fast spreading
* Polymorphic
* Metamorphic
* Transport vehicles
* Zero-day Exploit.

Virus Countermeasures:-

Anti-virus Approach:-

* the ideal soln to the threat of viruses is prevention: Do not allow a virus to get into the sys.

  > Detection
  > Identification
  > Removal

Four generations of anti-virus software:-

* First generation : simple scanners.
* Second " : heuristic "
* Third " : activity traps
* Fourth " : full-featured protection

Advanced Anti-virus Techniques:-

* More sophisticated anti-virus approaches & products continue to appear.

Generic decryption:-

This technology enables the anti-virus pgm to easily detect even the most complex polymorphic viruses, while maintaining fast scanning speeds.

> CPU Emulator

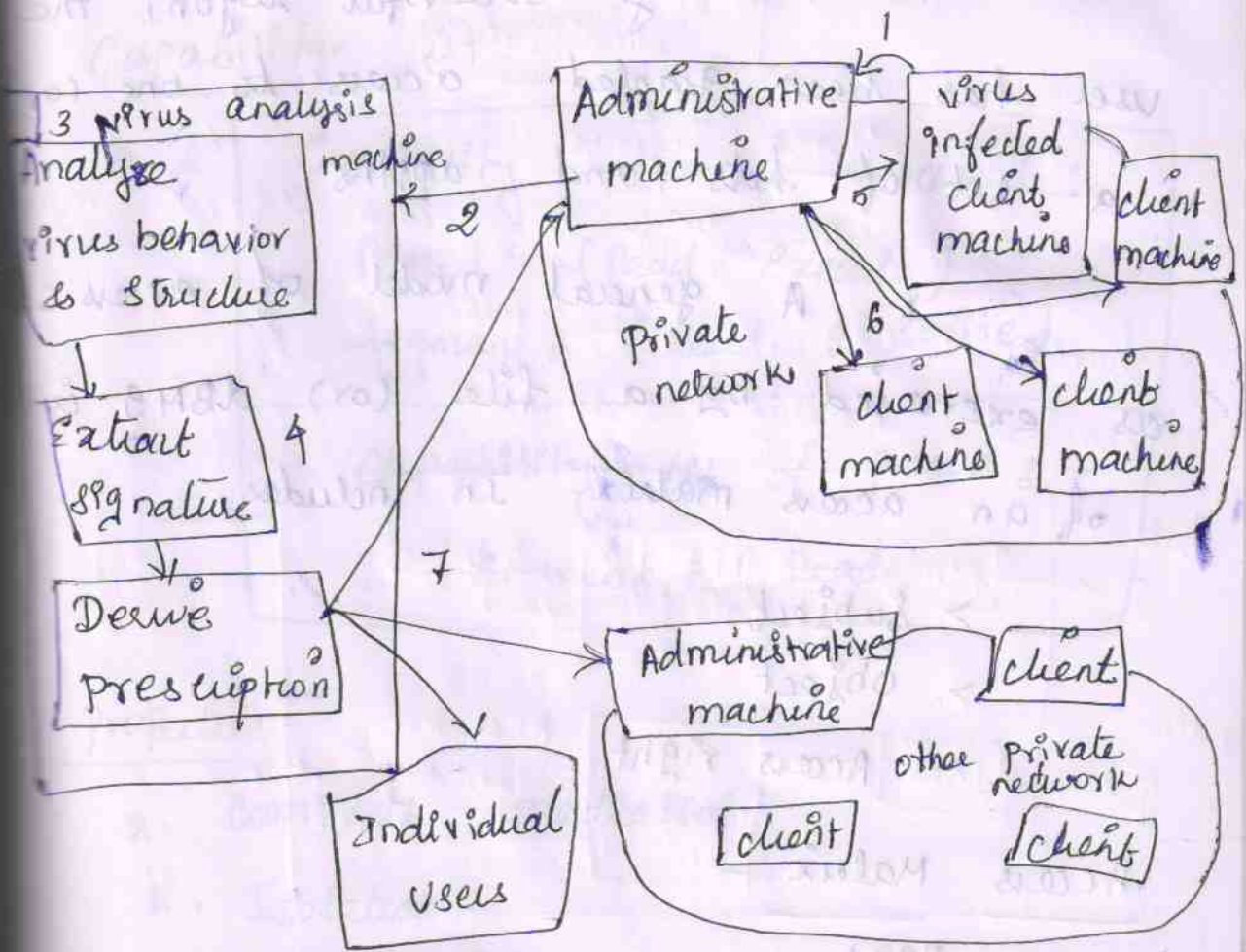
> Virus signature scanner

> Emulation ctl module.

Digital Immune System :-

* Integrated mail sys

* Mobile - Pgm systems.



Behavior - Blocking software :-

* Attempt to open, view, modify files

* " format disk drives

* Modification of logic.

Trusted Systems

* One way to enhance the ability of a sys to defend against intruders and malicious pgm is to implement trusted system technology.

Data Access ctrl :-

* Following successful logon, the user has been granted access to one (or) a set of hosts and applns.

* A general model of access ctrl as exercised by a file (or) dBMS is that of an access matrix. It includes,

> Subject
> Object
> Access right

Access Matrix :-

	Pgm1	...	Segment A	Segment B
Process 1	Read Execute		Read write	
Process 2				
:	.		.	

Access control list :-

Access control list of Pgm 1: Process 1 (Read, Execute)
Access control list of Segment A: process 1 (Read, Execute)
Access control list of segment B: Process 1 (Read, Execute)

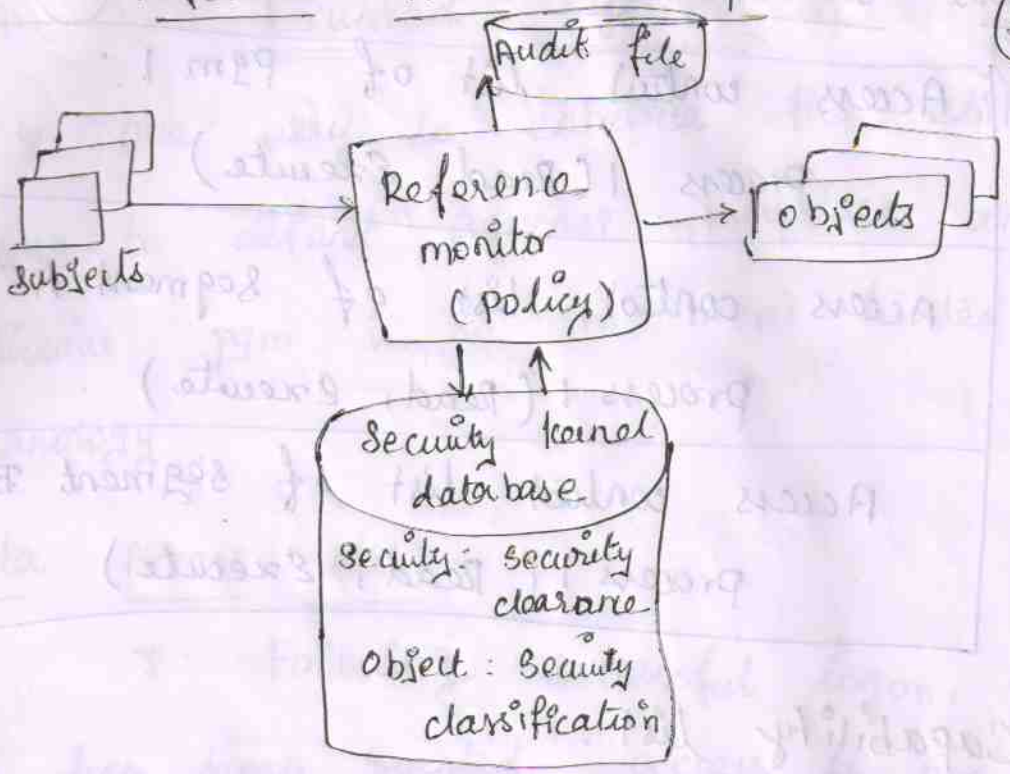
Capability list :-

Capability list of process 1: Pgm 1 (Read, Execute) Segment A (Read, Write)
capability list of process 2: Segment B (Read)

Properties:-

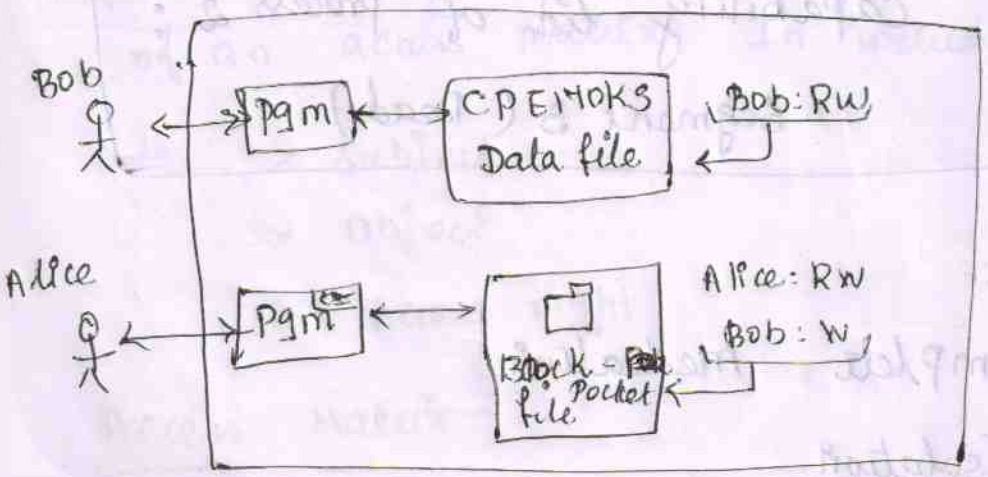
* Complete mediation
* Isolation
* Verifiability
* The reference monitor has access to a file, known as the "security kernel database".

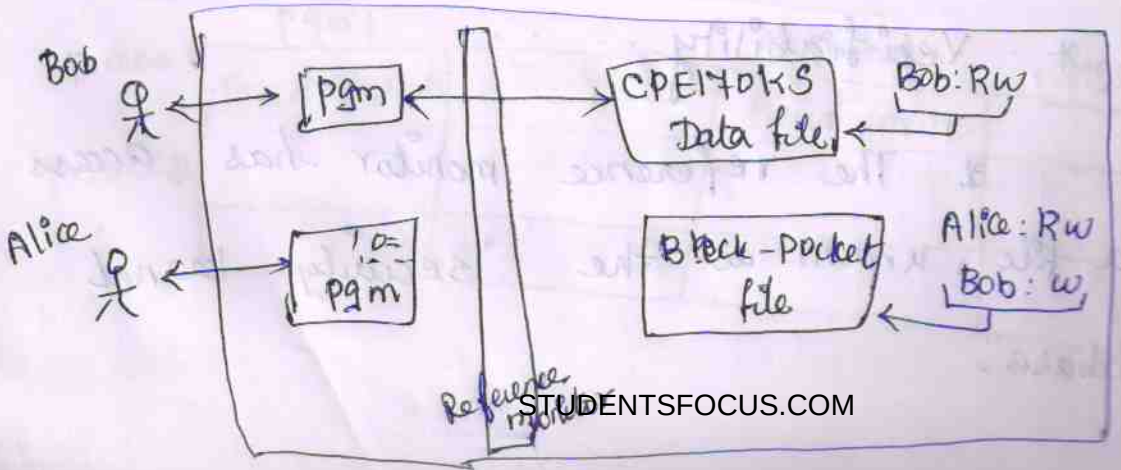
Reference Monitor concept:-

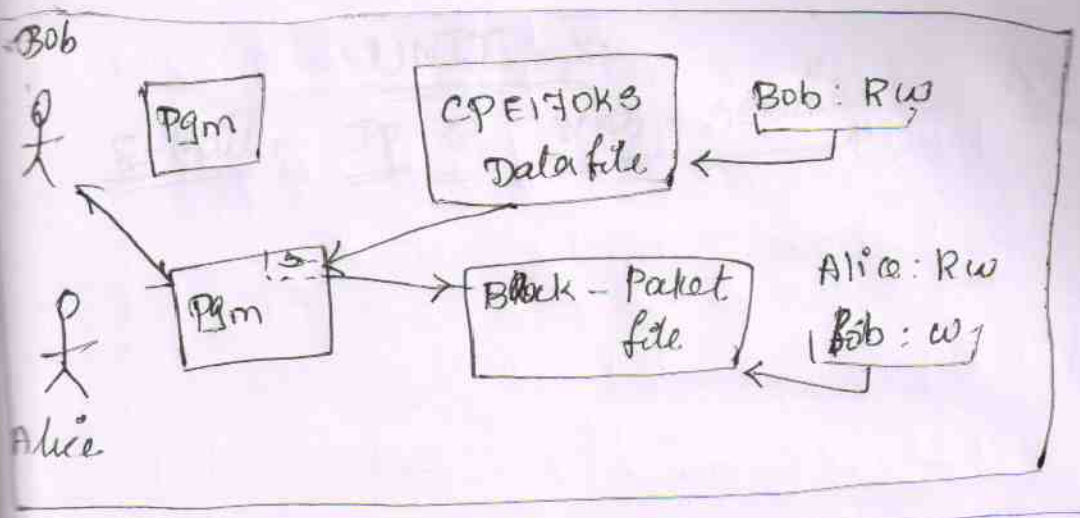


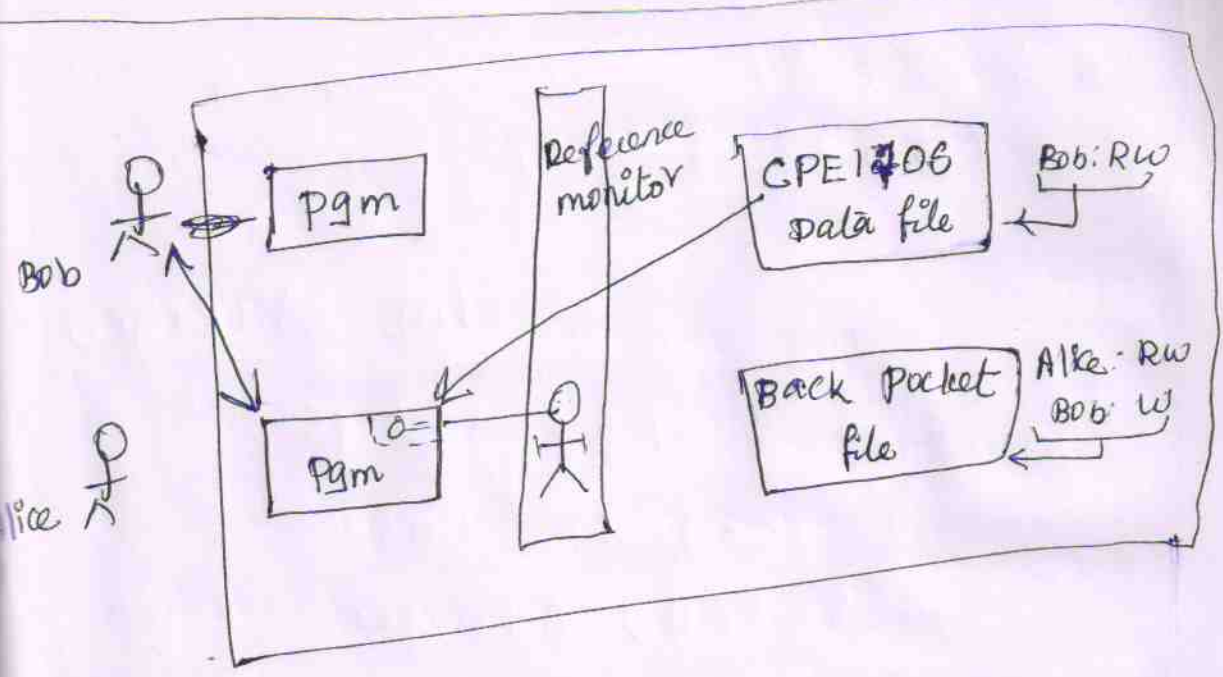
Trojan Horse Defense:-

* One way to secure against Trojan horse attacks is the use of a secure, trusted operating system.






Bob
Pgm
CPE170KS
Data file
Bob : Rw
Pgm
Back - Packet
file
Alice : Rw
Bob : w
Alice


Bob
Pgm
Reference
monitor
CPE170S
Data file
Bob: Rw
Back Packet
file
Alice: Rw
Bob: w
Pgm
Alice