PAM

PAM stands for pluggable authentication module

In the normal situaltion the users database are in the file
=> /etc/passwd
and
=> /etc/shadow

this file will be searched for login in the workstation. But the problem is when you are a network environment the login process needs to check something at somewhere else suppose you are running a IPA server or LDAP(Lightweight directory access protocol) server this login program needs a place to look for authentication information .Thats where PAM comes from .

With the use of PAM you can redirect any program to it and then it needs authentication.any application can redirect to PAM. PAM can work on authentication on any type of services.like if you want to authenticate with a private and public key pair,or you want to login with a USB stick or you want to authenticate with plain password,if you want to disable the root login PAM can used for all of this thing.

Then main advantage of Pam is that you can use PAM for anything. so if you want to implement strong authentication you should use PAM.

PAM modules are stored in the

/lib/security

the configuration file that shows how this module is going to work is located

/etc/pam.d.A system administrator can add or remove module to harden the security for different application.

For example the configuration for login is stored in the

=>/etc/pam.d/login

the configuration for samba is stored in the

=>/etc/pam.d/samba

There is a file caled **‘other’** that is empty and it is invoked if no service is selected

in the PAM configuration this pattern is followed

module-type control-flag module-path module-args

1) module-path is the module that is to run

2) module-args is the arguments that you want to be passed

there are a very few arguments.Actually most of the module have their own arguments

3) module-type refers different types of authentication different module-type is used for different types of authentication

→ **‘account’** is used for account verification checking weather the account has access or is the password is expired

→ **“auth”** does the second part it authenticate with the password

→ **“password”** is used for authentication update such as password update

→ “**session**” is used for keeping the session of the user

control flag is used for how the PAM respond if the authentication fails. response can be complicated or can be simple

the simple flag are the followes

→ **requisite**
→ **required**
→ **sufficient**
→ **optional**

if the flag is requisite then if the authentication failed the whole authenticationn process will stop immidietly

if the flag is required then if the authentication proces fail still the remaining module will still run

if the flag is suuficient before any module that means this module is enough for giving the authentication

if the flag is optional then it is not mandatory for the module to be successful unless it is the only module