

Plugged Authentication Module

ΚΟΤΖΑΝΙΚΟΛΑΟΥ ΠΑΝΑΓΙΩΤΗΣ

ΚΟΡΕΑΣ ΠΛΑΤΩΝ

Τι είναι το PAM ;

- ✓ ομάδα προγραμμάτων που αυθεντικοποιούν εκτελούνται μέσω άλλων προγραμμάτων
- ✓ τα PAM-aware προγράμματα λειτουργούν ως υπηρεσία και το βασικό καθήκον τους είναι ο έλεγχος ταυτότητας του χρήστη
- ✓ τα προγράμματα αυτά λειτουργούν ως ένα API υπηρεσιών συσχετιζόμενες με την αυθεντικοποίηση

Η λειτουργία του PAM

- ✓ Ο έλεγχος πρόσβασης πραγματοποιείται εκτός του περιβάλλοντος Kernel σε αντίθεση με την κλασική αυθεντικοποίηση των Linux
- ✓ Το PAM υποστηρίζει κοινόχρηστες βιβλιοθήκες για την κατασκευή μηχανισμών ελέγχου ταυτότητας οι οποίες βρίσκονται υπό του φακέλου (/lib/security)
- ✓ Οι εφαρμογές χρησιμοποιούν το module pam_authenticate για την αυθεντικοποίηση και το αρχείο /etc/pam.conf ή /etc/pam.d/ για την παραμετροποίηση
- ✓ Υπάρχουν πάνω από 70 μονάδες/modules PAM, η καθεμία με τις δικές της επιλογές και ανταποκρίσεις ως προς το σύστημα.
- ✓ Όλες οι μονάδες βρίσκονται μέσα στον φάκελο /lib/security

Πλεονεκτήματα του PAM

Ο διαχειριστής του συστήματος μπορεί να επιλέξει :

- ✓ τον προεπιλεγμένο μηχανισμό ελέγχου αυθεντικοποίησης για το σύστημα του.
- ✓ μέσα από μια μεγάλη γκάμα από μηχανισμούς αυθεντικοποίησης, από την χρήση ενός απλού κωδικού πρόσβασης μέχρι ένα σύστημα αναγνώρισης προσώπων
- ✓ να διαμορφώσει τον μηχανισμό ελέγχου ταυτότητας του χρήστη βάσει της εφαρμογής που επιθυμεί.
- ✓ πολλαπλούς κωδικούς πρόσβασης εάν κρίνεται απαραίτητο, για την επίτευξη υψηλότερης ασφάλειας
- ✓ την χρήση ενός module PAM χωρίς να αλλάξει τον βασικό μηχανισμό αυθεντικοποίησης του συστήματος

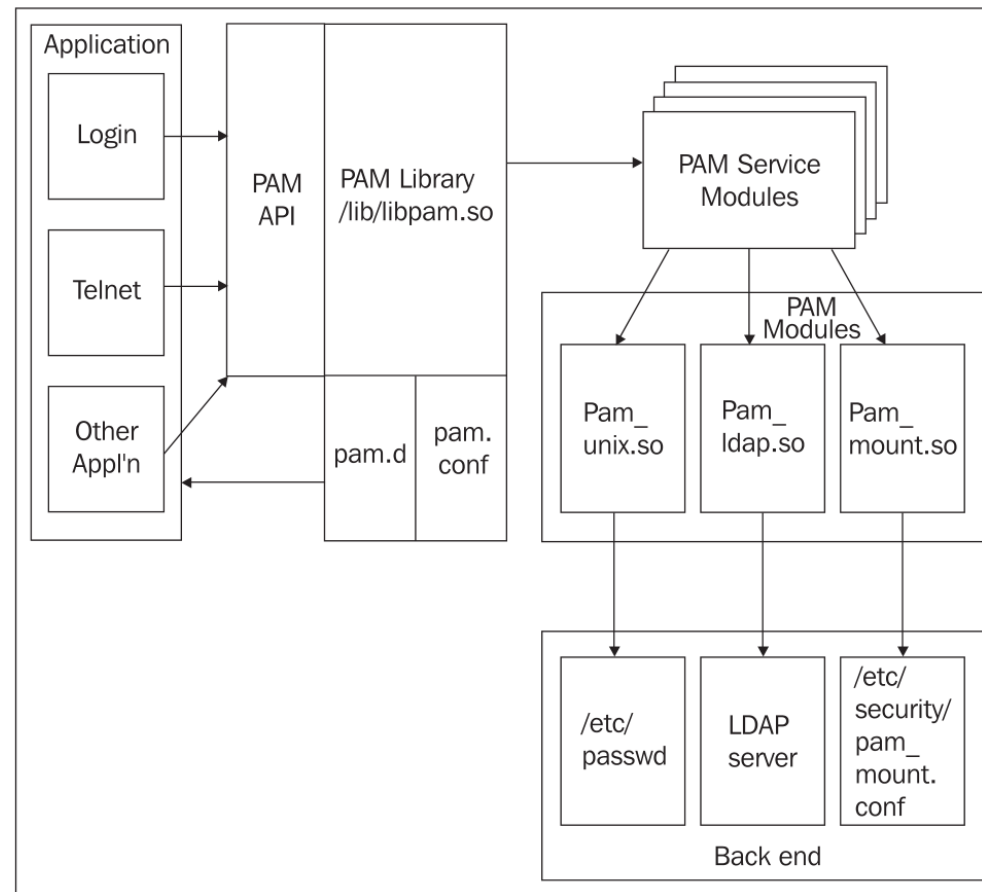
Υποθετικό παράδειγμα

1. Το πρόγραμμα X
2. χρησιμοποιεί ένα PAM module `/lib/security/foo`
3. Παραμετροποιείται από το αρχείο ρυθμίσεων του `/etc/pam.d/foo`
4. για να εκτελεστούν ενέργειες αυθεντικοποίησης Y

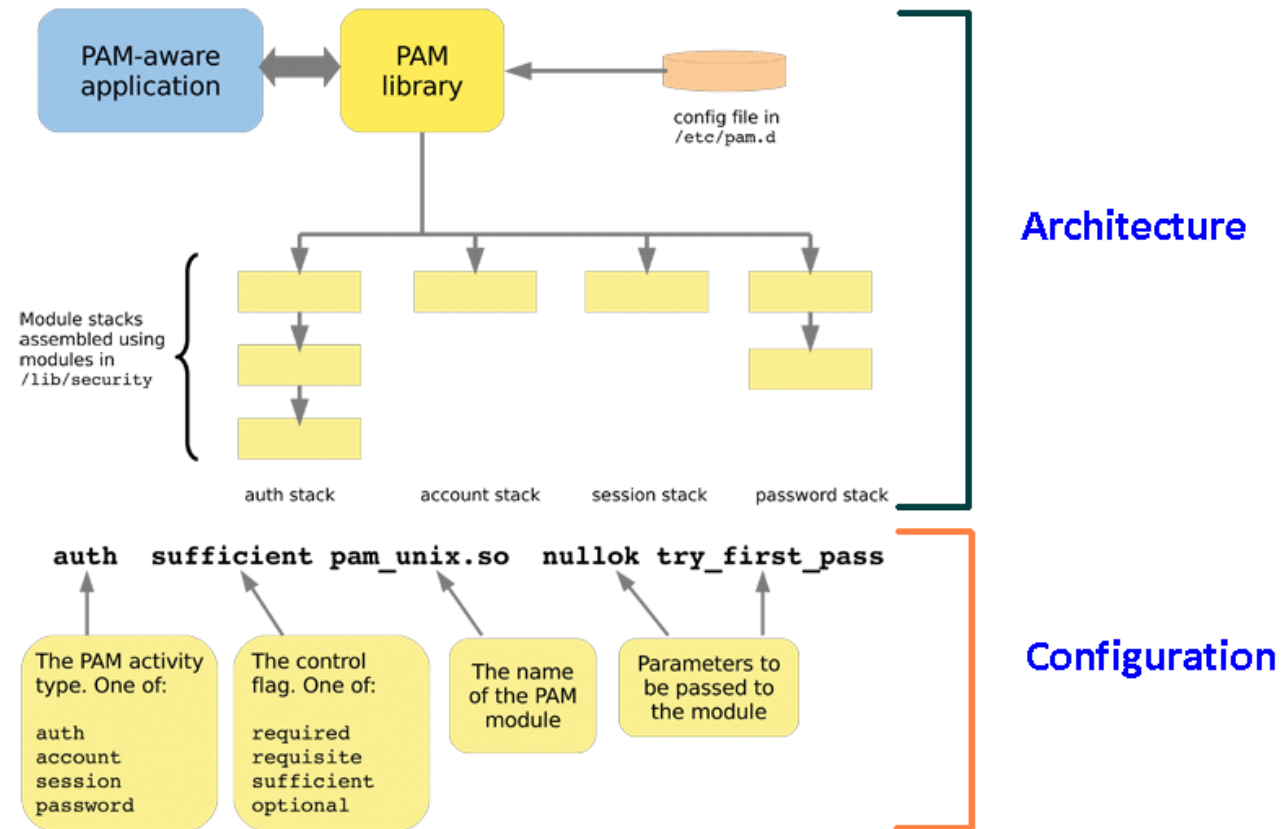
Κοινές μονάδες PAM

- ✓ `pam_cracklib` - αξιολογεί την ισχύ του συνθηματικού πρόσβασης
- ✓ `pam_issue` – προσθέτει προκαθορισμένο κείμενο κατά την σύνδεση του χρήστη
- ✓ `pam_nologin` – ελέγχει εάν υπάρχει `/etc/nologin`
- ✓ `pam_rootok` – ελέγχει εάν ο χρήστης είναι `root`
- ✓ `pam_securetty` - ελέγχει εάν η τρέχουσα `tty` είναι κατοχυρωμένη στο `/etc/securetty`
- ✓ `pam_time` - ελέγχει τον επιτρεπόμενο χρόνο μεταξύ των διαδοχικών συνδέσεων `/etc/security/time.conf`

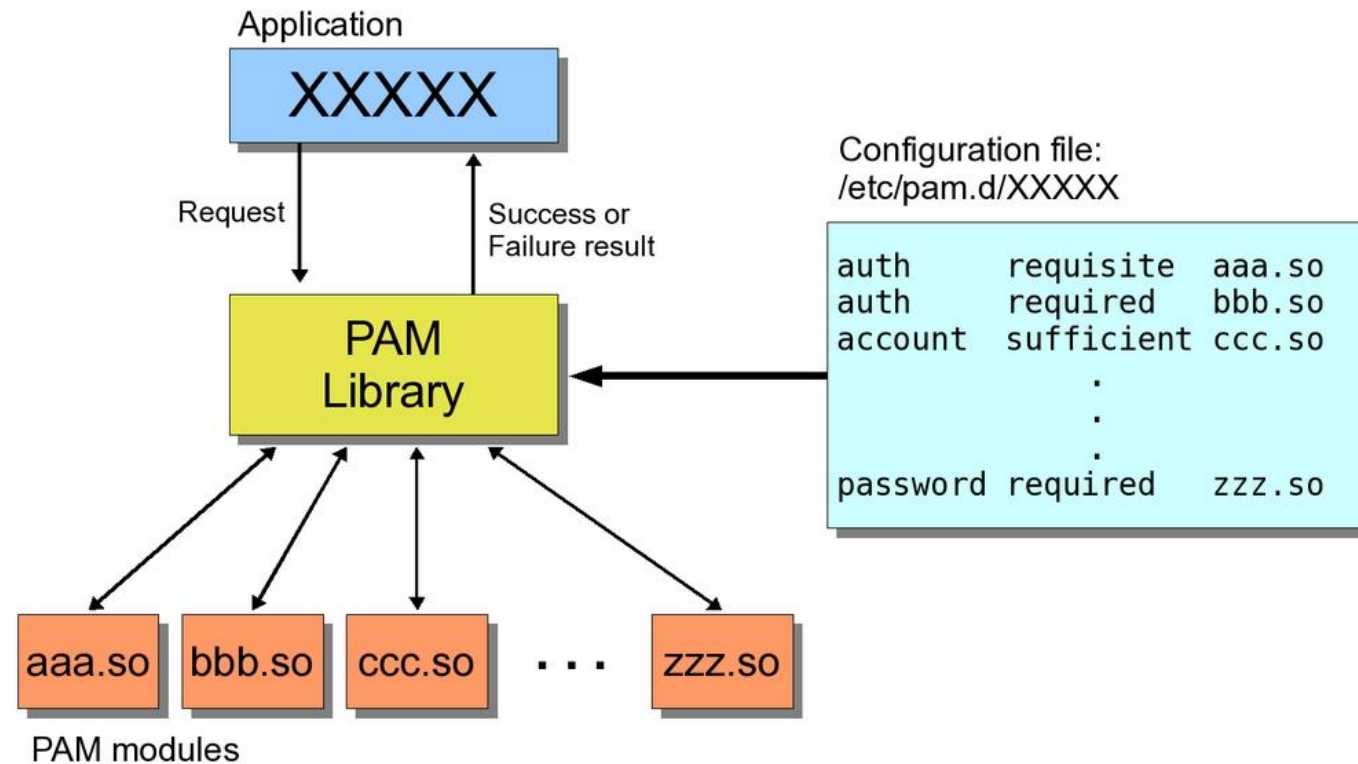
Αρχιτεκτονική PAM



Αρχιτεκτονική PAM



Αρχιτεκτονική PAM



Τύποι Διεπαφών των ΡΑΜ

✓ **Auth** : ελέγχει ποιος είναι ο χρήστης

(Λειτουργεί τόσο για τον έλεγχο του χρήστη μέσω του κωδικού του πρόσβασης όσο και για να παρέχει προνόμια στα μέλη μιας ομάδας/group.)

✓ **Account** : ελέγχει εάν επιτρέπεται η πρόσβαση στον λογαριασμό

(Εκτελείται ξεχωριστά από το σύστημα διαχείρισης χρηστών και συνήθως χρησιμοποιείται για το περιορισμό ή τη πρόσβαση σε μια υπηρεσία ανάλογα με την χρονική περίοδο μέσα σε μια ημέρα)

Τύποι Διεπαφών των ΡΑΜ

- ✓ **Password** : ελέγχει εάν έχει αλλαχθεί ο κωδικός και τον ενημερώνει για τον κάθε χρήστη
- ✓ **Session** : ελέγχει & διαχειρίζεται την συνεδρία σύνδεσης

(Λειτουργεί για να το υπάρχει έλεγχος σε υπηρεσίες κατά την συνεδρία του χρήστη όπως έλεγχος αρχείων καταγραφής)

Αρχείο ρύθμισης του PAM

Βρίσκεται το αρχείο ρύθμισης του PAM στο `/etc/pam.d` ή το `/etc/pam.conf`

service-name module-type control-flag module-path module-options

service-name : το όνομα της υπηρεσίας, μπορεί να είναι για παράδειγμα `su`, `ftp`, `login` ή `passwd` κτλ.

module-type : `auth`, `account`, `session` ,`password`

control-flag : η παράμετρος αυτή ελέγχει την συμπεριφορά του PAM module σε περίπτωση που θα επιτύχει ή αποτύχει η διαδικασία ελέγχου ταυτότητας. Τα control flags που χρησιμοποιούνται είναι τα `binding`, `include`, `optional`, `required`, `requisite` και `sufficient`

Αρχείο ρύθμισης του PAM

service-name module-type control-flag module-path module-options

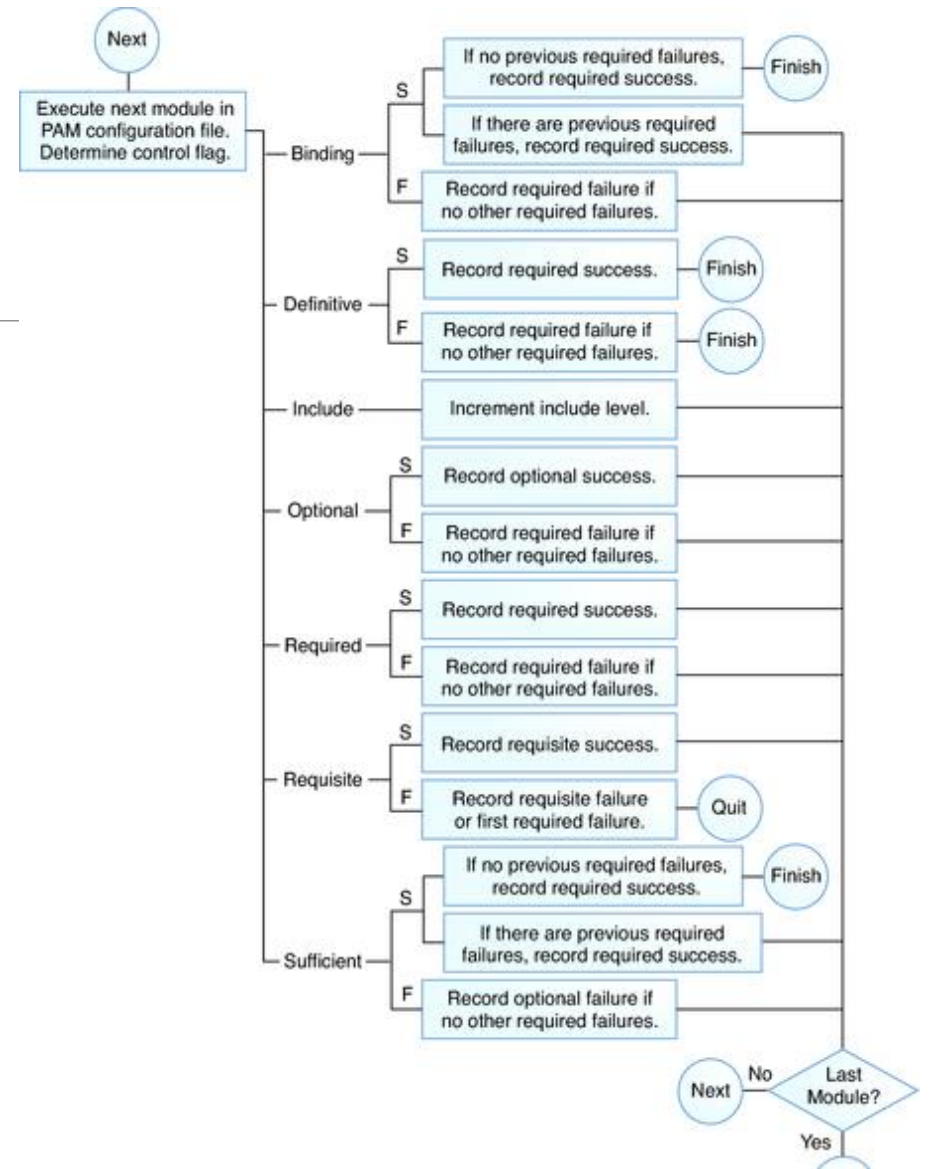
module-path: η παράμετρος αυτή οδηγεί στην διαδρομή προς το αντικείμενο της βιβλιοθήκης που υλοποιεί την υπηρεσία. Εάν η διαδρομή δεν είναι απόλυτη τότε θεωρείται ότι είναι σχετική με το με το /usr /lib /security

module-options : η παράμετρος αυτή μας δίνει την δυνατότητα να προσθέσουμε επιπρόσθετες επιλογές του module με βάση τον τρόπο κατασκευής του καθενός. Συνήθως περιλαμβάνουν την nowarn και την debug επιλογή.

Τιμές ελέγχου RAM

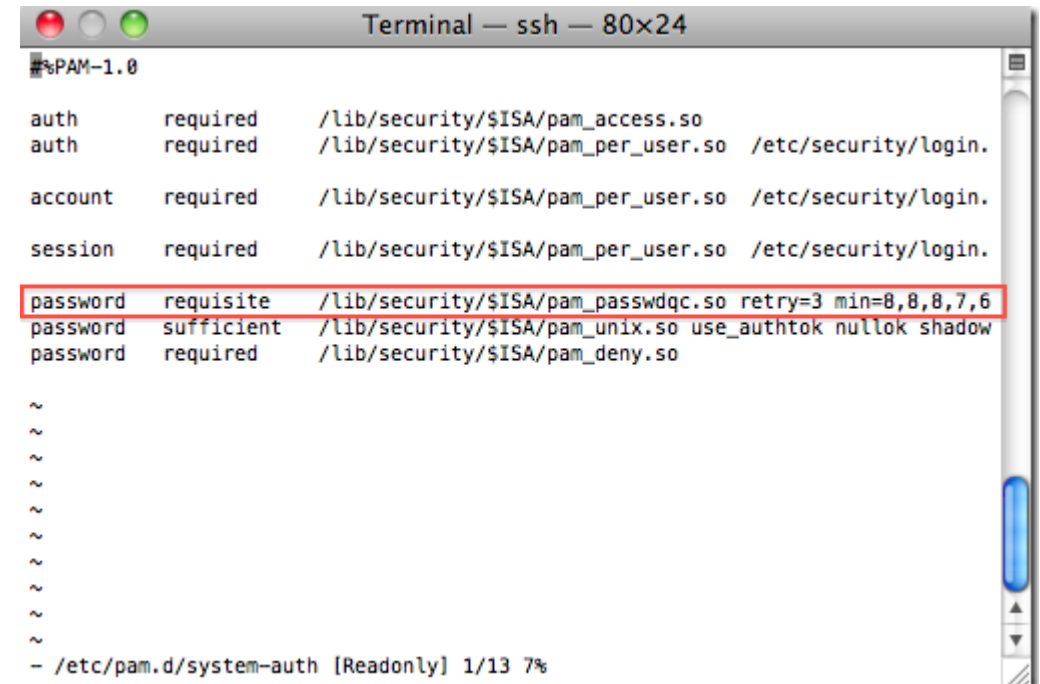
Τιμή	Επιτυχία εκτέλεση	Αποτυχία εκτέλεσης
requisite	Συνεχεία της εκτέλεσης	Διακοπή της εκτέλεσης
required	Συνεχεία της εκτέλεσης	Μήνυμα σφάλματος εφόσον όμως εκτελεστούν όλα τα υπόλοιπα modules
Sufficient	Σταματά η εκτέλεση εφόσον υπάρχει προηγούμενο module required με σφάλμα	Συνεχεία της εκτέλεσης
optional	Συνεχεία της εκτέλεσης	Συνεχεία της εκτέλεσης εφόσον όμως δεν υπάρχουν άλλα σφάλματα από τα υπόλοιπα modules

Λογικό διάγραμμα με την χρήση των τιμών ελέγχου PAM



Παράδειγμα για έλεγχο ισχυρών κωδικών πρόσβασης

```
~ # cat /etc/pam.d/system-auth
#%PAM-1.0
auth      required      /lib/security/$ISA/pam_access.so
auth      required      /lib/security/$ISA/pam_per_user.so /etc/security/login.map
account   required      /lib/security/$ISA/pam_per_user.so /etc/security/login.map
session   required      /lib/security/$ISA/pam_per_user.so /etc/security/login.map
password  requisite      /lib/security/$ISA/pam_passwdqc.so retry=3 min=8,8,8,7,6
password  sufficient    /lib/security/$ISA/pam_unix.so use_authok nullok shadow
password  required      /lib/security/$ISA/pam_deny.so
```

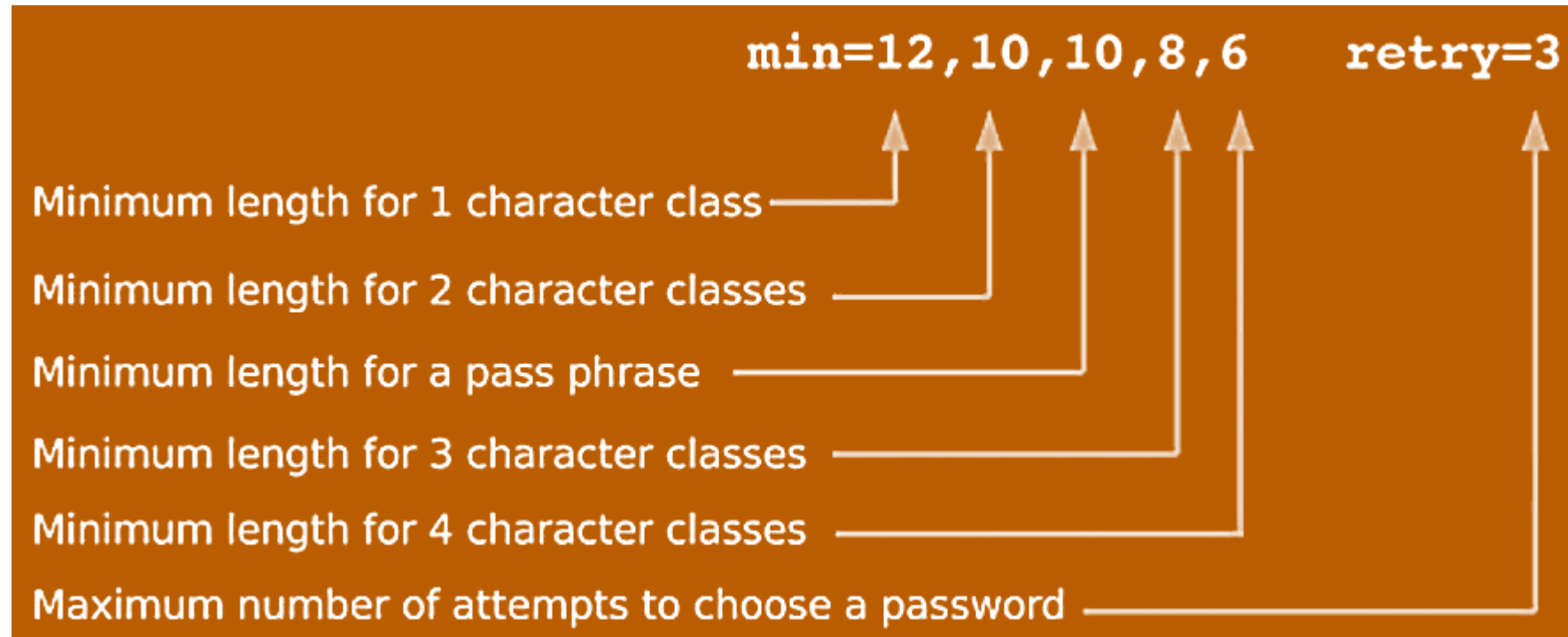


```
Terminal — ssh — 80x24
#%PAM-1.0
auth      required      /lib/security/$ISA/pam_access.so
auth      required      /lib/security/$ISA/pam_per_user.so /etc/security/login.
account   required      /lib/security/$ISA/pam_per_user.so /etc/security/login.
session   required      /lib/security/$ISA/pam_per_user.so /etc/security/login.
password  requisite      /lib/security/$ISA/pam_passwdqc.so retry=3 min=8,8,8,7,6
password  sufficient    /lib/security/$ISA/pam_unix.so use_authok nullok shadow
password  required      /lib/security/$ISA/pam_deny.so

~
~
~
~
~
~
~
~
~
- /etc/pam.d/system-auth [ReadOnly] 1/13 7%
```


Παράδειγμα για έλεγχο ισχυρών κωδικών πρόσβασης

password requisite pam_passwdqc.so min=12,10,10,8,6 retry=3



Βιβλιογραφία

Έντυπη

- ✓ Pluggable Authentication Modules, Packt Publishing

Ηλεκτρονική

https://docs.oracle.com/cd/E26502_01/html/E29015/pam-32.html

<http://www.linux-pam.org/Linux-PAM-html>

https://en.opensuse.org/openSUSE:Pam-face-authentication_project

https://linux.die.net/man/8/pam_passwdqc

<https://www.techrepublic.com/article/enforce-strong-passwords-with-pam-passwdqc/>