

UN' APPLICAZIONE PAM



Sistemi di Elaborazione dell' Informazione:
Sicurezza su Reti
Prof. Alfredo De Santis

a cura di :

Bettinelli Antonella
Capone Simonetta
Piccirillo Roberto

UN'APPLICAZIONE PAM

SOMMARIO



- INTRODUZIONE ←
- CENNI SU PAM
- L' APPLICAZIONE

UN'APPLICAZIONE PAM

INTRODUZIONE



I programmi che forniscono particolari servizi devono essere in grado di autenticare gli utenti.

L' autenticazione rappresenta, quindi, una prova di identità.

UN'APPLICAZIONE PAM

INTRODUZIONE



Esistono vari meccanismi che garantiscono l' autenticazione di un utente.

Ad esempio Unix identifica gli utenti attraverso l' immissione di una password e la verifica di questa mediante il confronto con quella (cifrata) presente nel file */etc/passwd*

UN'APPLICAZIONE PAM


PAM



PAM (Pluggable Authentication Modules) è un modo per permettere all' amministratore di sistema di creare un procedimento di autenticazione.

UN'APPLICAZIONE PAM

Scopo di PAM



Lo scopo di PAM è quello di separare lo sviluppo di software che richiede servizi di autenticazione, dalla scelta dei meccanismi di autenticazione.

UN'APPLICAZIONE PAM



Vantaggi di PAM

- Fornisce uno schema comune di autenticazione che può essere usato con un' ampia varietà di applicazioni.
- Permette grande flessibilità e controllo sull' autenticazione, sia per l' amministratore di sistema che per chi sviluppa le applicazioni.

UN'APPLICAZIONE PAM



Vantaggi di PAM

- Permette agli sviluppatori di applicazioni di implementare i propri programmi senza dover tenere conto di un particolare schema di autenticazione.

UN'APPLICAZIONE PAM



OBIETTIVO

Verrà mostrata la realizzazione di una applicazione che utilizza i moduli **PAM**.

L' applicazione effettua l' autenticazione degli utenti che intendono accedere ad un database.

UN'APPLICAZIONE PAM



Realizzazione

La realizzazione si articola in due fasi:

- Implementazione di un database di cui si vuole controllare l' accesso.
- Implementazione di una applicazione PAM-aware per l' autenticazione degli utenti.

UN'APPLICAZIONE PAM



SOMMARIO

- INTRODUZIONE
- CENNI SU PAM ←
- L' APPLICAZIONE

UN'APPLICAZIONE PAM



CENNI SU PAM

- Cos' è PAM
- I moduli
- Il file di configurazione
- Le applicazioni

UN'APPLICAZIONE PAM

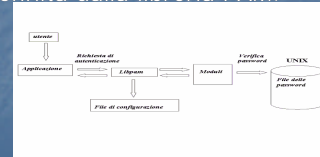
Cos' è PAM

PAM è un sistema che consente l'autenticazione utilizzando un insieme di librerie condivise (i moduli)



I moduli

Le applicazioni comunicano con i moduli caricati in memoria, presenti nel file di configurazione, tramite l' utilizzo di una API definita dalla libreria PAM.



I moduli (1)

Vi sono quattro tipi di moduli :

- **authentication** consentono di autenticare un utente mediante la richiesta di una password
- **account** verificano lo stato dell' account di un utente. Testano se esso è attivo oppure scaduto.

UN'APPLICAZIONE PAM

I moduli (2)

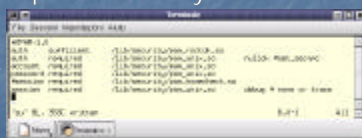
- **password** verificano lo stato dell' account di un utente. Testano se esso è attivo oppure scaduto.
- **session** consentono di definire delle azioni da compiere quando si accede e quando si esce dal sistema.

UN'APPLICAZIONE PAM

Il file di configurazione

La configurazione è suddivisa in più files, contenuti nella directory **/etc/pam.d** ed ogni servizio di autenticazione ha un proprio file in questa directory.

esempio del file di configurazione su

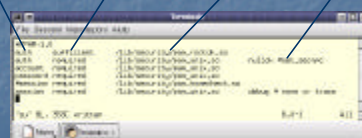


UN'APPLICAZIONE PAM

Il file di configurazione

Il file di configurazione può contenere una o più righe conformi alla seguente sintassi :

tipo_modulo livello_controllo path_modulo [argom_modulo]



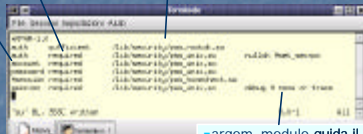
UN'APPLICAZIONE PAM

Il file di configurazione

■ **livello_controllo** indica il grado di attenzione per il modulo

■ **path_modulo** indica la posizione del modulo nel file system locale

■ **tipo_mod** indica uno tra i quattro tipi di moduli



■ **argom_modulo** guida il comportamento del modulo

UN'APPLICAZIONE PAM

Le applicazioni

Affinchè un' applicazione sia PAM_aware bisogna includere nel codice sorgente i seguenti files :

- **/lib/security/pam_appl.h**
- **/lib/security/pam_misc.h**

UN'APPLICAZIONE PAM

Le applicazioni

La linea di compilazione di una applicazione PAM_aware è la seguente :

cc -o applicazione -lpam -lpam_misc -ldl



UN'APPLICAZIONE PAM

Le applicazioni

Un' applicazione che fornisce servizi di autenticazione deve utilizzare le funzioni che la libreria **libpam** mette a disposizione.

La libreria carica dinamicamente i moduli presenti nel file di configurazione.

UN'APPLICAZIONE PAM

Le applicazioni

E' importante che l' applicazione tratti le funzioni come delle black-box, le quali si occuperanno di fornire i servizi di autenticazione.

UN'APPLICAZIONE PAM

SOMMARIO

- INTRODUZIONE
- CENNI SU PAM
- L' APPLICAZIONE ←

UN'APPLICAZIONE PAM

L' APPLICAZIONE

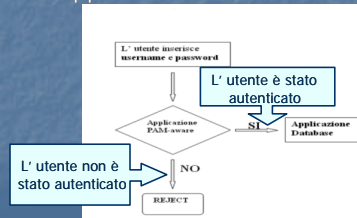
La presentazione verrà divisa in 2 parti

- Applicazione database
- Applicazione PAM-aware

UN'APPLICAZIONE PAM

L' APPLICAZIONE

Interazione dell' applicazione database con l' applicazione PAM-aware.



UN'APPLICAZIONE PAM

Il database

Il database è stato realizzato tramite la libreria di funzioni **gdbm** (GNU database).

UN'APPLICAZIONE PAM

GNU database

GNU gdbm è una libreria di routine che gestisce i file di dati che contengono coppie chiave/dato.

Le principali operazioni sono quelle di memorizzazione, di recupero e di cancellazione di una chiave.

UN'APPLICAZIONE PAM

L' applicazione database

Il database creato supporta le usuali operazioni di gestione:

- Creazione
- Rimozione
- Inserimento
- Ricerca
- Cancellazione
- Stampa

UN'APPLICAZIONE PAM

L' applicazione database

Viene riportata la parte di codice che richiama la funzione di autenticazione.

```
#include "database.h"
```

```
int main(int argc, char **argv)
{
    ...
    ...
    if(authenticazione(user))
        applet();
    return 0;
}
```

Viene invocata la funzione di autenticazione.
Se l'utente è stato autenticato viene invocata `applet()` che gestisce il database, altrimenti l'applicazione Termina.

UN'APPLICAZIONE PAM

L' applicazione PAM-aware (1)

```
int autenticazione(const char *user){
    ...
    retval=pam_start("database",user,&conv,&pamh);
    /*inizializza l'interfaccia e carica il file di configurazione*/
    if(retval==PAM_SUCCESS)
    /*la funzione termina */
        retval=pam_authenticate(pamh,PAM_AUTH_ERR)
    /*Richiama i moduli authentication presenti
    nel file di configurazione effettuando l' autenticazione */
    else{
        fprintf(stdout,"%s\n",pam_strerror(pamh,retval));
        return(0);
    /* viene stampato il motivo del fallimento e
    l' applicazione termina*/
    }
}
```

continua...

UN'APPLICAZIONE PAM

L' applicazione PAM-aware (2)

```
...if(retval==PAM_SUCCESS)
    retval=pam_open_session(pamh,0);
    /*Richiama i moduli di session presenti nel file di
    configurazione e apre una sessione per
    L' utente autenticato */
else{
    fprintf(stdout,"%s\n",pam_strerror(pamh,retval));
    return(0);
    /* Se la funzione non termina con successo
    viene stampato il motivo del fallimento e
    l' applicazione termina */
}
}
```

continua...

UN'APPLICAZIONE PAM

L' applicazione PAM-aware (3)

```
...
if(retval==PAM_SUCCESS){
    /*se l' operazione termina con successo si richiede l' eventuale
    cambio della password*/
    do{
        printf("Vuoi cambiare la password?...(s/n)...");
        fflush(stdout);
        fgets(input,1024,stdin);
        sscanf(input,"%c",&c);
    }while((c!='s' && (c!='S') && (c!='n') && (c!='N'));
    if((c=='s')||(c=='S'))
        retval=pam_chauthtok(pamh,0);
    /* richiama i moduli di gestione della password*/
    }else{
        fprintf(stdout,"%s\n",pam_strerror(pamh,retval));
        return(0);
    }
}
```

continua...

UN'APPLICAZIONE PAM

L' applicazione PAM-aware (4)

```
...
if(retval==PAM_SUCCESS){
    retval=pam_close_session(pamh,0);
    /*chiude la sessione dell' utente registrando eventuali
    informazioni nel file di log*/
}
else{
    fprintf(stdout,"%s\n",pam_strerror(pamh,retval));
    return(0);
}
if(retval==PAM_SUCCESS)
    fprintf(stdout,"%s\n",pam_strerror(pamh,retval));
}
```

continua...

UN'APPLICAZIONE PAM

L' applicazione PAM-aware (5)

```
...
if(pam_end(pamh,retval)!=PAM_SUCCESS){
    /*rilascia tutte le risorse detenute dall' applicazione */
    pamh=NULL;
    fprintf(stderr,"database ha fallito\n");
    return(0);
}
return (1);
}
```

UN'APPLICAZIONE PAM

Il file di configurazione

L' applicazione PAM-aware interagisce con il seguente file di configurazione.



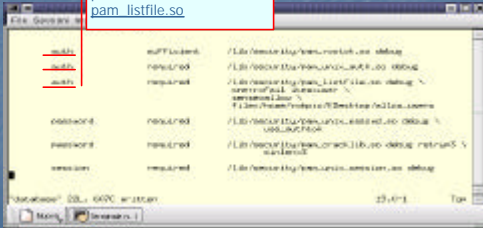
```
auth    sufficient /lib/security/pam_unix.so nullok
auth    required  /lib/security/pam_unix.so nullok
auth    required  /lib/security/pam_unix.so nullok
password    required /lib/security/pam_unix.so minlen=6
password    required /lib/security/pam_unix.so minlen=6
password    required /lib/security/pam_unix.so minlen=6
password    required /lib/security/pam_unix.so minlen=6
```

UN'APPLICAZIONE PAM

I moduli di autenticazione

I moduli di autenticazione utilizzati sono :

- [pam_unix_auth.so](#)
- [pam_rootok.so](#)
- [pam_listfile.so](#)

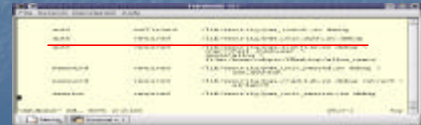


UN'APPLICAZIONE PAM

I moduli di autenticazione

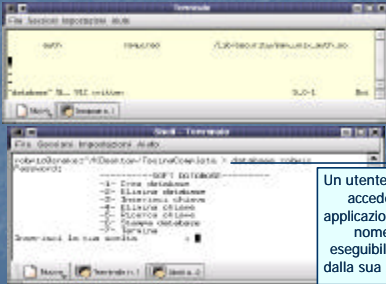
Il modulo **pam_unix_auth.so** autentica un utente nel seguente modo :

- richiesta della password
- confronto della password ottenuta con il file */etc/passwd* e */etc/shadow* se attivo



UN'APPLICAZIONE PAM

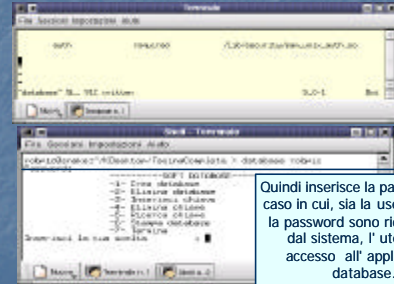
I moduli di autenticazione



Un utente che vuole accedere all'applicazione digita il nome dell'eseguibile seguito dalla sua username.

UN'APPLICAZIONE PAM

I moduli di autenticazione

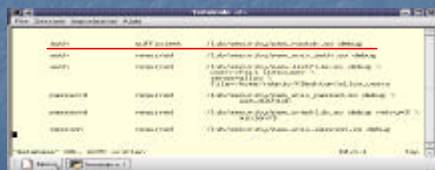


Quindi inserisce la password. Nel caso in cui, sia la username che la password sono riconosciute dal sistema, l'utente ha accesso all'applicazione database.

UN'APPLICAZIONE PAM

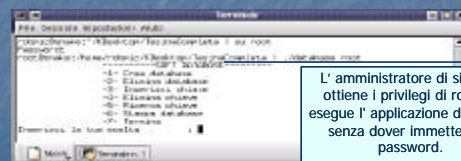
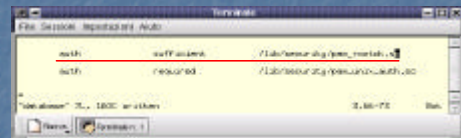
I moduli di autenticazione

Il modulo **pam_rootok.so** permette a tutti coloro che hanno i privilegi di root di non inserire la password.



UN'APPLICAZIONE PAM

I moduli di autenticazione

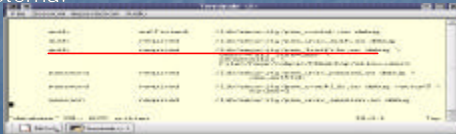


L'amministratore di sistema ottiene i privilegi di root ed esegue l'applicazione database senza dover immettere la password.

UN'APPLICAZIONE PAM

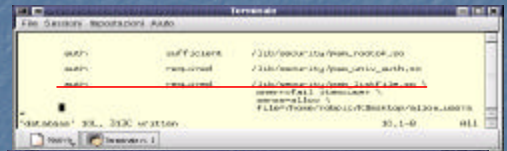
I moduli di autenticazione

Il modulo **pam_listfile.so** consente di limitare l'accesso all'applicazione a tutti gli utenti la cui username è registrata in un file creato dall'amministratore di sistema.



UN'APPLICAZIONE PAM

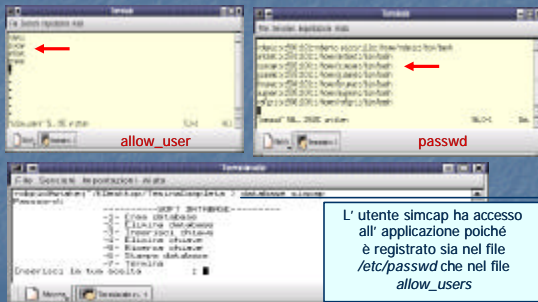
I moduli di autenticazione



L'utente simcap ha accesso all'applicazione poiché è registrato sia nel file /etc/passwd che nel file allow_users

UN'APPLICAZIONE PAM

I moduli di autenticazione



L'utente simcap ha accesso all'applicazione poiché è registrato sia nel file /etc/passwd che nel file allow_users

UN'APPLICAZIONE PAM

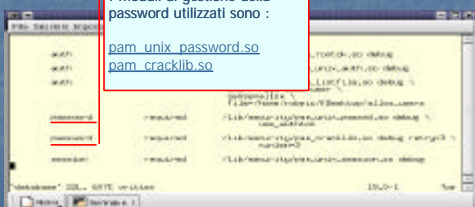
Gli argomenti di pam_listfile.so

- **onerr= fail** determina l'insuccesso del modulo in presenza di errori.
- **item=user** specifica il token su cui limitare l'accesso.
- **sense=allow** determina l'azione da quando il modulo ha successo.
- **file** indica il file sul quale bisogna effettuare il controllo.

UN'APPLICAZIONE PAM

I moduli di gestione della password

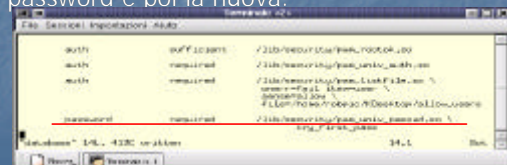
I moduli di gestione della password utilizzati sono :
[pam_unix_passwd.so](#)
[pam_cracklib.so](#)



UN'APPLICAZIONE PAM

I moduli di gestione della password

Il modulo **pam_unix_passwd.so** permette di modificare la password dell'utente, prima facendogli inserire la vecchia password e poi la nuova.



UN'APPLICAZIONE PAM

I moduli di gestione della password

L'utente simcap inserisce login e password.

Dopo essere stato autenticato dal sistema l'utente decide se vuole cambiare la password.

UN'APPLICAZIONE PAM

I moduli di gestione della password

Se la password inserita in precedenza è corretta viene richiesto l'inserimento della nuova password.

L'utente conferma la nuova password ed accede all'applicazione database.

UN'APPLICAZIONE PAM

I moduli di gestione della password

Gli argomenti passati sono:

Forza il modulo a settare la nuova password in sostituzione a quella memorizzata nel modulo delle password precedentemente caricato.

UN'APPLICAZIONE PAM

I moduli di gestione della password

Il modulo **pam_cracklib.so** controlla che le password non siano banali, ovvero

- palindrome
- simili o rotazione della vecchia password
- semplici
- già usate

UN'APPLICAZIONE PAM

I moduli di gestione della password

L'utente decide di modificare la password.

L'utente inserisce la nuova password che non viene accettata perché simile alla vecchia.

UN'APPLICAZIONE PAM

I moduli di gestione della password

L'utente inserisce la nuova password che non viene accettata perché troppo corta.

L'utente inserisce la nuova password che non viene accettata perché è una parola di dizionario.

UN'APPLICAZIONE PAM

