Logowanie kluczem USB

Bartosz Pieńkowski

16 września 2011

1 Założenia projektu

Celem projektu jest umożliwienie uwierzytelniania użytkowników systemu na podstawie kluczy USB posiadających unikalny numer seryjny.

Obecność urządzenia o numerze seryjnym przyporządkowanym do danego użytkownika eliminuje konieczność podawania przez niego hasła w procesie logowania.

Opcjonalnie weryfikacja może dotyczyć zarówno obecności klucza USB o żądanym numerze seryjnym, jak i poprawności hasła, co pozwala zwiększyć bezpieczeństwo systemu.

2 Mechanizm PAM

2.1 Zasada działania

Optymalnym rozwiązaniem kwestii uwierzytelniania jest wykorzystanie mechanizmu PAM[1] będącego zbiorem modułów oferujących różne metody uwierzytelniania, które można wykorzystać w wymagających tego aplikacjach.

Modularna architektura mechanizmu gwarantuje elastyczność w doborze metod uwierzytelniania dla każdej aplikacji z osobna, dokonywanym poprzez modyfikację plików konfiguracyjnych zlokalizowanych w katalogu `/etc/pam.d/`.

2.2 Moduł `pam_usbkey.so`

Realizacją założeń projektu jest dostarczenie modułu PAM implementującego uwierzytelnianie na podstawie numerów seryjnych podłączonych urządzeń USB. Założenia te spełnia moduł `pam_usbkey.so`.

W momencie zainicjowania procesu uwierzytelniania moduł ten odczytuje numer seryjny przypisany uwierzytelnianemu użytkownikowi z pliku konfiguracyjnego `usbkey.conf`.

[1] Pluggable Authentication Modules

Kolejnym krokiem jest uzyskanie listy obecnych w systemie urządzeń USB i porównanie przypisanych im numerów seryjnych z wartością odczytaną z pliku konfiguracyjnego. Uwierzytelnienie kończy się sukcesem w przypadku natrafienia na szukany numer seryjny, w przeciwnym razie rezultatem jest odmowa dostępu.

2.3 Konfiguracja

Każda aplikacja korzystająca z mechanizmu PAM posiada oddzielny plik konfiguracyjny w katalogu `/etc/pam.d/`, definiujący dobór modułów oraz wpływ wyniku ich działania na końcowy rezultat procesu uwierzytelniania.

Wymuszenie użycia modułu `pam_usbkey.so` jako wystarczającego do pomyślnego zakończenia procesu uwierzytelniania wymaga modyfikacji pliku `login` poprzez dodanie na szczycie stosu modułów linii:

```
auth      sufficient      pam_usbkey.so
```

Inną możliwością jest wykorzystanie modułu `pam_usbkey.so` razem ze standardową metodą uwierzytelniania hasłem, zaimplementowaną w postaci modułu `pam_unix.so`. W tym wypadku proces uwierzytelniania kończy się sukcesem jedynie w sytuacji, gdy obydwa moduły zakończą działanie z pozytywnym rezultatem.

Narzuca to konieczność uzupełnienia pliku `login` o następujące linie:

```
auth      required        pam_usbkey.so
auth      required        pam_unix.so
```

3 Instalacja modułu

Kompilacja kodu źródłowego oraz instalacja modułu w systemie odbywa się przy użyciu skryptu *Makefile*, poprzez wydanie kolejno poleceń:

```
make
make install
```

Za przywrócenie zawartości katalogu do stanu sprzed kompilacji odpowiada polecenie:

```
make clean
```

4 Plik konfiguracyjny

Plik konfiguracyjny modułu `pam_usbkey.so` przechowywany jest w katalogu `/etc/security/` pod nazwą `usbkey.conf`. Stanowi on przyporządkowanie numerów seryjnych urządzeń USB użytkownikom systemu.

Każda linia pliku składa się z pary `nazwa_użytkownika:numer_seryjny`. Przykładowy plik `usbkey.conf` wygląda zatem następująco:

```
pienkowb:F0CADC673DF2C8ED
kowalskj:066B0969C9ACEBE9
wysockip:2DE087A50A1B42D7
```

Istotną kwestią bezpieczeństwa jest nadanie plikowi ograniczonych praw dostępu w celu zapobieżenia jego modyfikacji przez osoby nieuprawnione. Aktualizacja pliku leży w gestii administratora systemu.

Literatura

[1] Hernberg P.: *User Authentication HOWTO*

[2] *Red Hat Enterprise Linux Deployment Guide*

[3] Geisshirt K.: *Development with Pluggable Authentication Modules*