

# RSBAC

## System obowiązkowej kontroli dostępu



Dariusz Dwornikowski

# Co to jest RSBAC ?

- Rule Set Based Access Control
- Projekt Open Source
- Łata na jądro GNU/Linux podnosząca stopień bezpieczeństwa w systemie
- RSBAC to *zestaw* modeli bezpieczeństwa

# O Projekcie



- www : [www.rsbac.org](http://www.rsbac.org)
- Początek jako praca magisterska Amona Otta
- Ostatnia stabilna wersja : 1.2.5.X

# Po co RSBAC ??

Brak kontroli dostępu w systemach \*NIX

- Swobodny model dostępu w UNIX (DAC)
  - Zbyt mała kontrola pojedynczego zasobu
  - Prawa tylko : write, read, execute
  - Ufać użytkownikowi ? -> NIGDY
  - Niemożność tropienia wrogich zachowań ( audit )
  - Przykład : jedna grupa – wszyscy równi ?

# Po co RSBAC ??

## Scentralizowana kontrola

- Konto root
  - Usługi działają na prawach roota
  - Błędy w kodzie programów
  - Absolutna kontrola
  - Zagrożenie dla systemu (exploits)
  - Dyskrecja, zaufanie
  - Uczciwość administratora

# Główne cechy RSBAC

- Modułarna budowa - elastyczność
- Implementacja na poziomie jądra
- Różne modele bezpieczeństwa
  - MAC (Mandatory Access Control)
  - ACL (Access Control Lists)
  - RC (Role Compatibility)
  - AUTH (Authentication)
  - PaX (Pageexec)
  - A także (DAZ, FF, JAIL, UM ...)

# Główne cechy RSBAC cd.

- Duże możliwości poprzez łączenie modułów
- Moduły niezależne od siebie
- Łatwo dodawać nowe moduły (REG)
- Rozbudowane narzędzia kontroli
- Tryb uczenia
- Osobna rola Security Officer (przeważnie uid 400) – rozdzielenie uprawnień

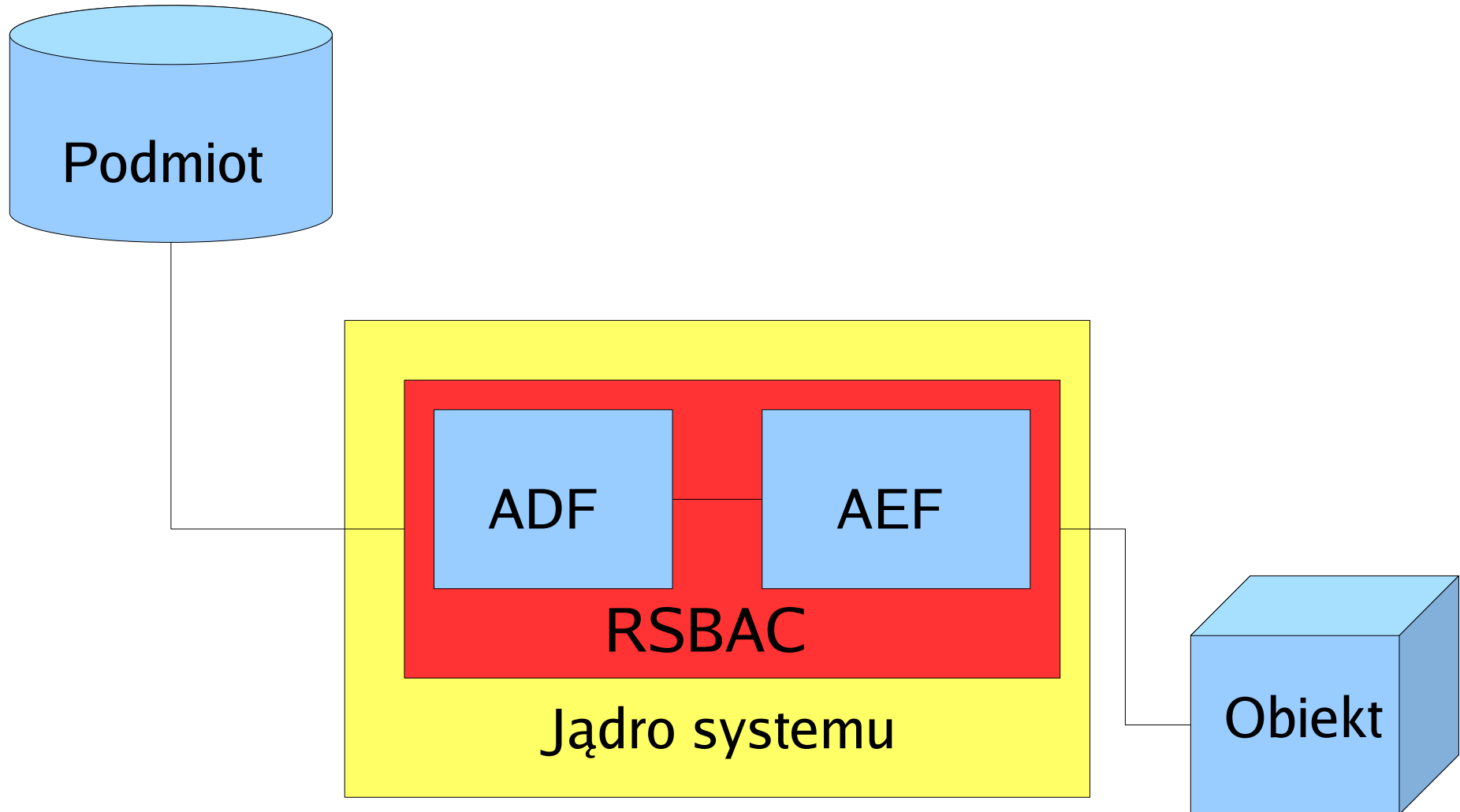
# Architektura RSBAC

Architektura RSBAC oparta jest na pojeciu Obiektu, Żądania oraz Podmiotu.

Przebieg autoryzacji przebiega następująco :

- Podmiot wysyła żądanie dostępu do obiektu
- ADF sprawdza czy podmiot może uzyskać dostęp ( GRANT )
- Podmiot dostaje przyzwolenie na dostęp do obiektu
- Lub odmowę. ( AEF – Access Enforcement Facility)

# Architektura RSBAC



# Architektura RSBAC

Podmiotem jest proces, uruchomiony na prawach użytkownika. Proces może być także podmiotem.

- Apache
- Sshd
- Ftpd
- Inne ...

# Architektura RSBAC

Obiektem można nazwać zasób, przykłady :

- FILE, DIR, FIFO, SYMLINK
- NETOBJ, NETTEMP, NETDEV
- IPC
- SCD ( System Control Data )
- USER, PROCESS
- DEV

# Architektura RSBAC

Przykłady żądań i obiektów :

- CHANGE\_OWNER ( DIR, PROCESS .. )
- CREATE (DIR, FILE ... )
- EXECUTE (FILE)
- READ, WRITE, DELETE (FILE, DIR ..)
- TRACE (PROCESS)
- BIND, CONNECT, LISTEN, SEND etc (NETOBJ)

# Przykład z “życia” - Apache

- Apache startuje na prawach roota
- Zrzuca prawa na rzecz użytkownika www
- Podatny na ataki, expolity
- W przypadku błędów w kodzie – zagrożenie całego systemu i innych usług
- Błędy w modułach podatnych na ataki (mod\_suexec, mod\_php etc.. )

# Przykład z “życia” - Apache cd.

## Zabezpieczenie z RSBAC

- Tworzymy role dla Apache
- Określamy *tylko te* zasoby, które są niezbędne
- Typy ( FILE, DIR, NETOBJ )
- Zamykamy go w pewnego rodzaju klatce
- Zapewniamy bezpieczeństwo

# Instalacja RSBAC

- Nałożenie łaty RSBAC na jądro Linux
- Instalacja pakietu rsbac-admin
- Założenie konta secoff z uid=400
- Reboot ...

Pierwsze uruchomienie spowoduje utworzenie polityki, która umożliwi booting systemu, jednakże zalogowanie się nie będzie możliwe ( AUTH ).

# Parametry jądra

- `rsbac_softmode` ( brak wymuszania zasad bezpieczeństwa )
- `rsbac_auth_enable_login` ( wymusza `auth_may_setuid` na `/bin/login` )
- `rsbac_auth_learn` ( tryb uczenia modułu AUTH )
- `rsbac_acl_learn` ( tryb uczenia modułu ACL )
- `rsbac_debug_all` ( tryb debugowania )
- ...

# Narzędzia użytkownika

- rsbac\_menu ( przyjazny tryb użytkownika w formie menu )

```
RSBAC Administration Tools v1.2.5
root@t43: RSBAC Administration

Main FD Menu

User Attributes:          Go to user attribute menu
Group Attributes:        Go to Linux group attribute menu
File/Dir Attributes:     Go to file/dir attribute menu
Block/Char Device Attributes: Go to dev attribute menu
Process Attributes:      Go to process attribute menu
Network Device Attributes: Go to Network Device attribute menu
Network Template Definition: Go to Network Template Definition menu
Network Template Attributes: Go to Network Template attribute menu
RC Roles:                Go to RC role menu
RC Types:                Go to RC type menu
ACL Management:          Go to ACL menu
ACL Group Management:    Go to ACL group menu

-----
Settings:                RSBAC menu settings
Logging:                 Setup general logging
Switch Modules:          Switch modules on or off
Switch Softmode:         Switch global or module softmode

-----
Check Status:            rsbac_check 1 1
Show Status
Show RC Status
Show ACL Lists
Show ACL Groups
Show eXtended Status

-----
Bash Shell
-----
Quit

< OK >          <Cancel>          < Help >
```

# Narzędzia użytkownika

- rsbac\_\* ( wiele narzędzi CLI )
- moduł\_\* ( narzędzia dla modułów )

Tylko secoff może zmieniać polityki. Możliwe jest jednak zdefiniowanie innych ról administratora bezpieczeństwa.

# Inne systemy bezpieczeństwa dla Linux

- Security Enhanced Linux (SELinux)
- Grsecurity
- Apparmor
- ACLs
- Linux Capabilities
- LIDS, Tripwire, Snort
- ...

# Podsumowanie

- Modułarna budowa
- Elastyczność
- Wysokie bezp.
- Ogromne możliwości
- Różne modele bezp.
- Darmowy
- Niezależny
- Trudna administracja
- Mało dokumentacji
- Trudne wdrożenie
- Koszt (???)

Dziękuję

Pytania ??