

# open



USE



IMPROVE



EVANGELIZE

開  
放  
的  
열린  
مفتوح  
libre  
मुक्त  
ಮುಕ್ತ  
livre  
libero  
ముక్త  
开放的  
açık  
open  
nyílt  
•••••  
πικρ  
オープン  
livre  
ανοικτό  
offen  
otevřený  
öppen  
открытый  
வெளிப்படை

## RBAC

Dariusz Ankowski



# O potrzebie bezpieczeństwa

- Wiadomo. Dane.
- Jeśli [seti@home](#), to moje, a nie włamywacza z .tw.



# Tradycyjny model bezpieczeństwa

- ZU – zu może, co może.
- Root – może wszystko.
- su – możesz być, kim zechcesz.
- sudo – możesz udawać, że jesteś kim zechcesz.



## Czy root to aby nie za dużo?

- Jeśli ZU musi zrobić coś, co może tylko root, czy musi mieć dostęp do roota?
- Czy root musi móc tyle, ile może? A może może móc mniej?



## Wejście sudo

- Pozwala na przydzielenie zu pewnych przywilejów do komend.
- Po właściwej konfiguracji daje szeroki wachlarz możliwości.



# Czemu więc RBAC?

- RBAC to coś więcej.
  - Autoryzacje
  - Profile
  - Role
  - API
  - Gotowa, bardzo bogata konfiguracja.
  - Przywileje.
  - Profilowane powłoki.
  - Ograniczone (restricted) powłoki.



# Autoryzacje

- Szczegółowo zdefiniowana możliwość wykonania pewnego zadania w systemie.
- Dotyczą pojedynczych elementów.
- Znacznie lepsza ziarnistość niż w sudo.



## Profile

- Autoryzacje zebrane w “portfel”.
- Definiują wyższe poziomy zarządzania systemem.
- Na przykład: Software Installation.
- Profile można przypisać profilom.



## Role

- Abstrakcyjni użytkownicy.
- Ograniczony dostęp (konieczność wykonania su z uprzywilejowanego konta).
- Możliwość przypisania profilowanej powłoki.
- Wielu użytkowników może mieć tę samą rolę.
- Mogą mieć wiele profili.



## Przykłady profili

- Primary Administrator
- Software Installation
- Printer Administrator



## Przykład roli

- Konto root w OpenSolaris.



## Profilowane powłoki

- pfsch
- pfcsh
- Znoszą konieczność wykonywania komend za pomocą pfsch.



# API

- Kod aplikacji może sprawdzać, czy użytkownik ją wykonujący ma odpowiednie uprawnienia.
- Bardzo drobna ziarnistość autoryzacji.

Przykład kodu z cron:

...

```
if (chkauthattr(CRONADMIN_AUTH, login_authchk) ||
```

...



## Przywileje

- Kod chcący uzyskać dostęp do uprzywilejowanego portu potrzebuje atrybutu `PRIV_NET_PRIVADDR`
- Alternatywa dla `SETUID`



# Ograniczone powłoki

- rsh
- Uniemożliwia zmianę ścieżki PATH.

# open



USE



IMPROVE



EVANGELIZE

## Thank you!

<XXX Name>  
<XXX Title>  
<XXX Email>  
<XXX Blog>

“open” artwork and icons by chandan:  
<http://blogs.sun.com/chandan>

開  
放  
的  
열린  
مفتوح  
libre  
मुक्त  
ಮುಕ್ತ  
livre  
libero  
ముక్త  
开放的  
açık  
open  
nyílt  
•••••  
πικρ  
オープン  
livre  
ανοικτό  
offen  
otevřený  
öppen  
открытый  
வெளிப்படை