

АДМІНІСТРУВАННЯ СИСТЕМ РОЛЬОВОГО РОЗМЕЖУВАННЯ ДОСТУПУ

Л. В. Степаненко¹, О. Є. Архипов¹

¹ Національний технічний університет України «Київський політехнічний інститут»

Анотація

В роботі розглядається модель адміністрування систем рольового розмежування доступу, проблеми, пов'язані з нею та способи їх вирішення

Ключові слова: політика безпеки, права доступу, роль, рольове розмежування доступу

Вступ

Будь-яка модель розмежування доступу є формалізованою математичною моделлю, майже завжди така модель є досить загальною і потребує доопрацювання і певних уточнень для того, щоб її можна було впровадити у реальній системі захисту інформації. Модель рольового розмежування доступу не є винятком. Відтак правила функціонування цієї моделі є загальними. У багатьох випадках в літературі надаються лише можливі підходи до вирішення певних проблем, при цьому не надається конкретних методів вирішення.

Отже коли ведеться практична розробка системи розмежування доступу, постає задача деталізації формальної моделі розмежування доступу. Саме в цей момент виникає необхідність в усуненні неточностей та доопрацюванні формальної моделі розмежування доступу. Тобто основною метою є розробка такої моделі, що буде адекватною реальним обставинам функціонування системи і буде максимально їх враховувати.

Одним з кількох аспектів рольових моделей розмежування доступу, що потребують уточнення, є комплекс питань пов'язаних з адмініструванням у моделі рольового розмежування доступу. У такій моделі вводиться ієрархія адміністративних ролей, які мають права, необхідні для керування функціонуванням розмежування доступу. Складність адміністрування у цій моделі полягає у тому, що на користувачькі ролі накладені певні обмеження, зокрема обмеження, що накладаються на них вимогами ієрархії ролей. Отже при внесенні змін адміністраторами системи, ці обмеження обов'язково мають враховуватися, адже у іншому випадку може зустрітися ситуація, коли порушується ієрархія ролей користувачів, а отже ставиться під загрозу коректність функціонування системи розмежування доступу в цілому. Також запропоновано методи адміністрування у моделях рольового розмежування доступу з урахуванням ієрархії ролей.

1. Модель адміністрування систем РРД

Основні елементи базової моделі РРД включають в себе:

- U – множина користувачів
- R – множина ролей
- P – множина прав доступу до об'єктів комп'ютерної системи
- S – множина сесій користувачів
- $PA : R \rightarrow 2^P$ – функція, що визначає для кожної ролі множину прав доступу; при цьому для кожного $p \in P$ існує $r \in R$ така, що $p \in PA(r)$
- $UA : U \rightarrow 2^R$ – функція, що визначає для кожного користувача множину ролей, на які він може бути авторизований
- $user : S \rightarrow U$ – функція, що визначає для кожної сесії користувача, від імені якого вона активована
- $roles : S \rightarrow 2^R$ – функція, що визначає для користувача множину ролей, на які він авторизований у даній сесії; при цьому в кожен момент часу для кожного $s \in S$ виконується умова $roles(s) \subseteq UA(user(s))$.

При побудові такої моделі множини U , R , P і функції PA , UA лишаються незмінними в часі. В реальних же системах такий стан речей є неприйнятним, адже в процесі функціонування системи відбувається її розвиток та еволюція, користувачі можуть приймати на себе нові ролі, а існуючим ролям можуть знадобитися нові привілеї. Для реалізації можливості динамічного внесення змін в систему рольового розмежування доступу доцільно розглянути модель адміністрування РРД, побудовану на основі базової моделі РРД [1, 2, 3].

На додачу до елементів базової моделі РРД у моделі адміністрування РРД розглядаються наступні елементи:

- AR – множина адміністративних ролей ($AR \cap R = \emptyset$)
- AP – множина адміністративних прав доступу ($AP \cap P = \emptyset$)
- $APA : AR \rightarrow 2^{AP}$ – функція, що для кожної адміністративної ролі визначає множину адміні-

того, щоб подолати цю проблему, задамо функцію $can - revoke(ar)$ так: $\forall ar : can - revoke(ar) = R$. Отже, фактично дозволимо будь-якій адміністративній ролі виключати будь-яку роль з множини авторизованих ролей користувача. Слід зазначити, що це надає адміністративним ролям занадто широкі права і залишає відношення часткового порядку лише відносно включення ролей до множини авторизованих ролей користувача. Це значно звужує придатність використання таких моделей РРД.

Удосконаленням методу каскадного виключення є так зване непряме каскадне виключення [2, 3]. Введемо функцію $can - revoke - indirect : AR \rightarrow 2^R$, що визначає для кожної адміністративної ролі множину ролей, які можуть бути виключені з множини авторизованих ролей користувача при каскадному виключенні з використанням даної адміністративної ролі, у разі, коли виникає суперечність $r \in can - revoke(ar), r' \notin can - revoke(ar)$.

Тобто з використанням адміністративної ролі $ar \in AR$ можливо виключити роль $r \in R$, таку, що існує $r' \in R, r' \geq r, r' \notin can - revoke(ar)$ з множини авторизованих ролей користувача тоді і тільки тоді, коли $r' \in can - revoke - indirect(ar)$. Таким чином ми обмежуємо права адміністративної ролі по виключенню ролей з множини авторизованих ролей користувача шляхом визначення функції $can - revoke - indirect(R)$.

Обмежене вилучення накладає на адміністративну роль наступне обмеження: дозволяється виключати лише таку роль $r \in R, r \in can - revoke(ar)$ з множини авторизованих ролей $UA(u)$ користувача $u \in U$, для якої не існує ролі $r' \in R$ такої, що $r' \geq r, r' \in UA(u)$.

Рівноправне додавання і виключення є частковим випадком методу обмеженого виключення, різниця складається в тому, що на ролі які можуть бути виключені з множини авторизованих ролей користувача даною адміністративною роллю додатково накладається умова: $can - revoke(ar) = can - assign(ar)$.

До переваг цих методів над методами, що базуються на каскадному виключенні, можна віднести більш простоту реалізації.

Висновки

Системи рольового розмежування доступу набувають значної популярності у зв'язку зі своєю ефективністю, але сучасні моделі РРД не передбачають динамічного внесення змін до системи. В такому випадку система РРД розширюється і доповнюється, створюються механізми адміністрування РРД. За своїм призначенням адміністративні ролі поділяються на 3 групи:

- Адміністрування множин авторизованих ролей користувачів
- Адміністрування множин прав доступу, якими володіють ролі
- Адміністрування ієрархії ролей

Але в базовій моделі адміністрування виникають протиріччя, що зменшують ефективність роботи адміністраторів. Запропоновано й розглянуто наступні способи їх вирішення:

- Каскадне виключення
- Непряме каскадне виключення
- Обмежене виключення
- Рівноправне додавання і виключення

Перелік використаних джерел

1. Hwai-Jung Hsu, Feng-Jian Wang A delegation Framework for task-Role based Access Control in WFMS.// Institute of computer Science and Engineering National Chiao Tung Iniversity./ Journal of Information Science and Engineering — 2011 — release 27 — c.1011–1028.
2. Toahchoo Iray On the formal analysis of spatio-temporal RBAC model. //Department of computer Science Colorado State University.
3. Li Fen, Liu Quan The application of RBAC in digital rights management system. // School of Information Engineering Wuhan University of Technology./ 2010 Ninth International Symposium on distributed and application to Business and Science.
4. Девянин П.М.Обзорные лекции по моделям безопасности компьютерных систем. //Прикладная дискретная математика./ Институт криптографии, связи и информатики — Москва. — 2009. — Вып.2 — с.152