РОЛЬОВЕ КЕРУВАННЯ ДОСТУПОМ

Role-Based Access Control (RBAC)

-принцип розподілу повноважень
-повноваження - право здійснювати певну дію над усіма об'єктами системи або їх підмножиною
-повноваження - сукупність елементарних операцій
-роль відповідає функції, дії або множині дій
-розподіл повноважень між ролями
-користувач може виконувати декілька ролей
-принцип найменших привілеїв
-не визначено механізм передачі прав між користувачами

Роль - суб'єкт системи, з яким пов'язаний несуперечливий набір повноважень, необхідних для виконання тих чи інших дій в системі.

Приклади:
Ролі користувачів в Windows і СКБД (призначаються через групи)
Приклад повноважень - оператори SQL в СКБД

RBAC практично реалізується із застосуванням контрольних механізмів дискреційного (ACL) або мандатного (мітки контекстів) керування доступом

Модель рольового керування доступом

U – множина користувачів
R - множина ролей
P – множина повноважень
S – множина сесій (сеансів)
Стан системы — {***U, R, P, S***}

Відображення:
$\boldsymbol{F_{PR}}$: $\boldsymbol{P \times R}$ (повноваження х ролі)
$\boldsymbol{F_{UR}}$: $\boldsymbol{U \times R}$ (користувачі х роли)
$\boldsymbol{F_{UR}}$ може бути реалізовано як матриця, рівень допуску або на основі дозволених тематик

Активні користувачі системи:
f_{user} : $\boldsymbol{S \rightarrow U}$ – користувач $u \in U$ здійснює даний сеанс s $\in S$ роботи в системі ($u=f_{user}(s)$)

Активні ролі сеанса (авторизовані ролі)/ активні ролі користувача:
f_{roles} : $\boldsymbol{S \rightarrow R}$ – набір ролей $\overline{R} \subset R$ із доступних користувачу та активних в даному сеансі ($\overline{R}=f_{roles}(s)$)

$f_{permissions}$: $\boldsymbol{S \rightarrow P}$ – набір повноважень $\overline{P} \subset P$, доступний користувачу по всім ролям, активним в даному сеансі ($\overline{P}=f_{permissions}(s)$)

Критерій безпеки системи рольового доступу - система вважається безпечною, якщо будь-який користувач u, що працює в сеансі s, може здійснювати дії, що вимагають повноваження p, тільки якщо $P= f_{permissions}(s)$, $p \in P$
Безпека рольових ситем керування доступом строго не доводиться!

Скільки і яких ролей може бути призначено для роботи з системою одному користувачеві ($\boldsymbol{F_{UR}}$)?
Скільки і які ролі може одночасно задіяти один користувач в одному сеансі роботи з системою (f_{roles})?
Можливі відносини між ролями?
Можливість делегування (передачі) прав від одних ролей іншим?

Функції авторизації:

$\pi 1$ (u, R) – чи може користувач u відкрити сеанс в ролі R
$\pi 2$ (s, p) – чи дозволено користувачеві у поточному сеансі виконувати дію (чи є дозвіл на p (P))

*можуть існувати ролі, на які не авторизовано жодного користувача

Різновиди рольових моделей:

-ієрархія ролей (частковий порядок)
-несумісні ролі:
--користувач не може мати несумісні ролі (ролі, що виключають одна іншу)
--несумісні ролі не можуть відкривати сеанси одночасно
--несумісні в одному сеансі ролі
-кількісні обмеження:
-на кількість користувачів, авторизованих на роль
--кількість сесій
--кількість повноважень в ролі
--кількість ролей, які мають деяке право

-зміна множини ролей
-зміна множини повноважень
-зміна ієрархії ролей (видалення ролей)

-з адміністративними ролями (повноваженнями)

Ієрархічна організація ролей

- Строгий листовий підхід - листовим ролям призначаються набори повноважень, що не перетинаються (неможливість призначення деяких повноважень двом ролям)
- Листовий підхід - повноваження отримують тільки листові ролі; старші ролі об'єднують підлеглі ролі (успадкування знизу), можливий перетин повноважень листових ролей
- Змішаний листовий підхід - старші ролі можуть включати додаткові в порівнянні з підлеглими ролями повноваження

Несумісні (взаємовиключні) ролі

$\overline{R}=f_{exclusive}(r)$ – для кожної ролі задає набір несумісних ролей

Статичний розподіл обов'язків

Заборона на надання певного набору прав або повноважень одному працівникові
(Зменшення ймовірності злочинних дій над критичними ресурсами)
Виконання таких дій потребує спільне виконання двома або більше користувачами

Окремий випадок - користувач може мати не більше двох ролей
* Заборона стосується облікових записів користувачів!

Динамічний розподіл обов'язків

Критичні операції не можуть виконуватися одночасно одним працівником (можливо, в одному сеансі)
Взаємовиключні на один сеанс ролі $f_{exclusive}$ ***(r)***

* Такий підхід може посилювати мандатні моделі керування доступом
* Варіант реалізації взаємоблокування

Кількісні обмеження по ролям

- Максимальна кількість повноважень, що може бути в ролі
- Обмеження кількості користувачів, які можуть отримати деяку роль

* Обмеження дозволяють спростити адміністрування системи

Групування ролей і повноважень

Перевірка логічної структури ролей (логічного покриття повноважень) або цілісності ієрархії, логічно пов'язаної групи повноважень або ролей, які мають бути наявні одночасно

Безпека рольових моделей контролю доступу строго не доводиться!

Індивідуально - групове керування доступом
(Спрощена рольова модель)

Робочою групою називається сукупність користувачів ІС, об'єднаних єдиними правами доступу до об'єктів і (або) єдиними привілеями (повноваженнями) виконання певних процедур обробки даних.

Група не є суб'єктом (не може ініціювати процес)
Не враховуються сеанси
Відношення $\boldsymbol{F_{UG}}$ на множинах користувачів та груп
Відображення f_{groups} ***(p) користувач***-групи та f_{users} ***(p)*** група -користувачі

Права доступу = індивідуальні + групові

Властивість безпеки в групових і рольових моделях не доводиться !!!

Модель рольового та групового доступу - *методика проектування і управління* дискреційними системами розмежування доступу при великій кількості користувачів, об'єктів і операцій доступу.

У реальних сценаріях права і привілеї не є незалежними, тобто є відношення часткового порядку

Можлива вкладеність груп, коли групи і користувачі входять у групи
(Тобто група - це список, а не контейнер)
Група надає свої права а також усіх батьківських груп

Відношення «входження» на множині груп (частковий порядок)
(Група може входити відразу в декілька груп)
-транзітівность
-рефлексівность
-антісімметрічность

→ Граф довільного виду, але без циклів

Ефективні права (підсумкові) = індивідуальні + групові, явні + успадковані ч-з контейнер

Якщо є мультиваріантність отримання прав — потрібна можливість явної заборони
(Користувач в групі, з якої його виключити не можна)

Рішення: обмежене членство (фільтри успадкування) або явна заборона з високим пріоритетом

Проблеми:
-надмірність / дублювання прав
-транзитівності відносин
-складність алгоритмізації

Аналіз і оптимізація індивідуально - групових систем керування доступом
(Теоретико - графова модель систем індивідуально - групового керування доступом до ієрархічних об'єктів)

Варіативність в наданні прав:
-Явні дозволи
-Спадковані дозволи
-Групові дозволи

Кількісні параметри ефективності призначення прав: **Кдубл** (менше дублювання)

→ Порівняння різних варіантів політик (порівняння кількості сутностей або призначень при різних моделях управління)

Завдання моделювання:
Аналіз близькості робочих груп
Злиття схожих груп
Автоматична класифікація

Коментарі до лекції:

Наступний клас моделей, які ми розглянемо - Рольові моделі керування доступом (RBAC).

В багатьох інформаційних джерелах із захисту інформації згадуються "в комплекті" дискреційні, нормативній та рольові моделі керування доступом і це створює враження, нібито ці три класи моделей становлять "альтернативу" одна до одної.
(я не раз глузував зі слова "альтернатива", наприклад, https://resheto.net/yumor/968-anekdot-pro-alternativu)
Згадується стара реклама по TV: "При всем богатстве выбора - другой алтернативы нет".
Тобто, обирати можливо з декількох варіантів, проте не всі результати нас задовольнять.
І лише один з варіантів буде "оптимальним". При цьому створюється ілюзія вибору.

І не тільки такі паралелі "дискреційне або нормативне або рольове" дають хибні уявлення про різні можливі підходи до керування доступом.

Дискреційне та нормативне керування доступом мають своє втілення в архітектуру купи різних ОС.
(Як записано в одному з перших стандартів безпеки ОС - керування доступом може бут реалізовано або на основі списків контролю доступом об`єктів (дискреційне у чистому вигляді) або на основі міток об`єктів (через мітки може бути реалізовано не лише нормативне керування, а й інші моделі).

Дискреційне керування доступом є самодостатнім, тобто його достатньо для втілення будь-якого призначення прав доступу суб`єктів на об`єкти, а нормативне керування, як правило, працює "поверх" дискреційного, бо дає загальну картину призначення, яка може бути уточнена завдяки ACL (але лише в сторону звуження прав).

Рольове керування доступом, як мінімум, працює на більш високому рівні, ніж перші дві моделі, та не має під собою ніяких низькорівневих механізмів системи. RBAC можливо розглядати або як схему та підхід до побудови системи керування доступом, або як алгебраїчний апарат, що дозволяє описувати системи керування доступом.

(2) У постановці рольової моделі визначаються множини ролей, які (по необхідності) можуть ще розкладатися на окремі повноваження. Користувачі (суб`єкти системи) авторизовані на якусь множину ролей та можуть входити в систему, тобто відкривати один або більше сеансів (але також можуть в якийсь момент часу не мати сеансів). Поточний стан системи визначається кортежем множин $\{U,R,P,S\}$.

Двостороннє відображення *FPR* дозволяє з`ясувати, яку підмножину повноважень включає деяка роль, або, в іншому напрямку, в якій підмножині ролей є деяке повноваження. Двостороннє відображення *FUR* дозволяє з`ясувати, яка підмножина користувачів має деяку роль, або, навпаки, на яку підмножину ролей авторизований деякий користувач. Тобто, ці два відображення можуть використовуватися як функція, що повертає різні типи результатів в залежності від типу даних аргументу.

Для активних користувачів системи (тих, що мають відкриті сеанси) функції *fuser, froles, fpermissions* за ідентифікатором сеансу s повертають, відповідно, ідентифікатор користувача, підмножину активних В ДАНОМУ СЕАНСІ ролей та підмножину доступних в даному сеансі (по всім активним ролям) повноважень.

Критерій безпеки RBAC системи ніяких властивостей системи не перевіряє, а лише стверджує, що система є безпечною, якщо користувачу будуть доступні лише ті повноваження, що визначаються відповідною функцією. (щось на кшталт "Якщо все робити вірно - то все буде добре:) І це лише набір позначень, за допомогою яких можливо описати логіку роботи деякоі систми з RBAC.

(3) Деталі поведінки системи в рольовій моделі будуть виглядати як обмеження (додаткові умови) до загальної постановки задачі.

В RBAC моделях можливо описати сценарії, в яких існують виключення (несумісність)
-між ролями, що належать одному користувачеві
(Користувач не може бути авторизований на деяку підмножину ролей, тому що вони "несумісні" між собою);
-між повноваженнями, що входять до однієї ролі;
-між ролями, що активовані в системі;
-між ролями, що можуть бути активовані одним користувачем у всіх його сеансах;
-між ролями, що можуть бути активовані в одному сеансі;
-між повноваженнями, що можуть бути активовані в системі;
-між повноваженнями, що можуть бути активовані одним користувачем у всіх його сеансах;
-між повноваженнями, що можуть бути активовані в одному сеансі;
А також багато іншого...

При необхідності, в запису RBAC моделі можуть використовуватися функції авторизації, що дають відповідь, чи може деякий користувач в поточний момент часу відкрити сеанс з декою роллю або чи може деякий користувач в поточний момент часу використовувати деяке повноваження.

(4) Окрім означених вище випадків обмежень з несумісністю ролей або повноважень, можливі RBAC моделі з кількісними обмеженнями ролей або повноважень.

Існує цілий клас моделей RBAC з ієрархічною побудовою дерева ролей (та, можливо, повноважень). Тобто, система ролей/повноважень має представлення у вигляді дерева. Таке представлення дає можливість зробити систему ролей/повноважень більш логічною та надає підхід до її перевірки на повноту і несуперечність. Як наслідок, при зміні множини ролей/повноважень виникає необхідність збереження цілісності дерева ролей/повноважень.

Також можливі моделі RBAC з адміністративними ролями - ролями, які мають "владу" над іншими ролями, повноваженнями або користувачами, тобто можливість зміни відповідних властивостей інших об`єктів.

(5) Ієрархія ролей може мати такі особливості:
-Суворий листовий підхід: кожне повноваження зустрічається лише в одні ролі (практично побудувати систему з таким розподілом повноважень майже неможливо);
-Листовий підхід: Дерево ролей, де більш загальні ролі складаються з детальних ролей, але набори повноважень у різних ролей можуть перетинатися (таке реально реалізувати, дає логічну побудову системи ролей).
-Змішаний листовий підхід: загальні ролі окрім детальних ролей можуть мати додаткові повноваження;
(Не знаю, навіщо таке будувати, мабуть, якщо не вдалося привести систему ролей до цілком логічної конструкції, то хоча б максимально наблизити до такої).

Несумісність (взаємовиключення) між ролями задається відповідною функцією, яка повертає для кожної ролі підмножину несумісних ролей або для пари ролей повертає булеве значення (або 0/1).

*Можна побачити, що дане представлення рольової моделі має багато варіативних позначень, які можуть використовуватись за необхідності. Крім того, в принципі, модель цілком допускає за необхідності розширення нотації (системи позначень).
Але при цьому введення додаткових функцій або позначень має бути логічно обгрунтованим і доцільним лише в разі, коли неможливо обійтись наявною системою позначень. Більш того, можливе існування багатьох інших представлень рольової моделі.

Статичний розподіл ролей/повноважень передбачає їх призначення незалежно від поточного стану системи (відкритих сеансів).

(6) Динамічний розподіл - можливість співіснування набору ролей/повноваженьв одному сеансі системи (або у всіх сеансах системи).

До речі, через конструкції взаємовиключення можливо представити розподіл повноважень між окремими обліковими записами (коли критичний набір привілей не може бути наданий одному користувачеві/обліковому запису).
А через динамічне взаємовиключення можливо логічно представити ситуацію ексклюзивного виконання деякого набору дій лише одним суб`єктом або взаємоблокування.

(7) Наявність груп користувачів дає можливість логічного групування облікових записів в залежності від виконуваних функцій користувачів та колективного призначення прав. Група не є суб`єктом системи.

*в моделі керування доступом Windows кожна група має унікальний SID, а користувач (його маркер доступу) має декілька SID (у томи числі SIDи груп) і кожний з SID може надавати користувачеві деякі дозволи/привілеї.

В разі наявності груп, права доступу будуть складатися з явно призначених користувачеві та отриманих через групи, до яких він входить та успадкованих від об`єктів вищого рівня.

Вже має бути відомим термін "ефективні дозволи" - такий набір дозволів, який користувач в поточний момент часу фактично зможе отримати на деякий об`єкт доступу. Але особливості реалізації механізмів керування доступом у ОС Windows не мають ускладнювати загальну теорію.

(8) В реальних системах не все є логічним та продуманим. Скоріш за все, це наслідок нашарування деякої послідовності ідей та концепцій, що використовувалися в різні періоди часу в процесі еволюції різних версій даної ОС.

Практично можливе відношення часткового порядку між правами та повноваженнями. Також можлива вкладеність груп, коли одна група повністю включає права доступу іншої групи. Такі реалії роблять представлення системи груп/ролей/повноважень доволі складним.

(9) Застосування підходів, які визначені в рольовій моделі керування доступом, дає можливість формалізації та логічного опису стану деякої системи керування доступом, її перевірки на логічну повноту і несуперечність, а також подальшої оптимізації (модифікації за деяким критерієм). Наприклад, виявлення надмірностей або дублювання прав.

Враховуючи співіснування одночасно багатьох механізмів надбання прав доступу (явних, групових, спадкових), може бути розроблено декілька схем реалізації системи керування доступом. В цьому випадку використання підходів з моделей RBAC знов таки дає можливість їх логічного порівняння. Критерієм порівняння може бути складність реалізації (наприклад, штрафні бали за введення додаткових груп, тощо), або коефіцієнт дублювання (одночасного надбання деяким суб`єктом тих самих прав з різних джерел - явні, групові, успадковані). За такими критеріями можливе порівняння різних схем призначення прав доступу або їх реалізацій.

Також задача аналізу системи розмежування доступу відкриває можливість для застосування різних підходів до аналізу близькості робочих груп, розбиття або злиття груп та застосування методів автоматичної класифікації.

Питання і вправи:

Класифікація моделей рольового керування доступом.
Функції авторизації в моделях рольового доступу.
Характеристики моделей рольового керування доступом.
Перевірте, чи можливо в нормативній або дискреційній моделі керування доступом емулювати рольове керування доступом і навпаки.

Формальна постановка задачі рольового керування доступом.
Приклади додаткових умов (обмежень):
Ієрархія ролей
Несумісні ролі
Обмеження по ролям
Групування ролей
Індивідуально - групове розмежування доступу

Завдання рольового керування доступом зі статичним розподілом обов'язків (користувач не може мати деякі ролі разом)
Завдання рольового керування доступом з динамічним розподілом обов'язків (деяка роль не може бути активована в двох і більше сеансах)
Завдання рольового керування доступом з ієрархічною організацією ролей. Види ієрархії ролей в моделях RBAC.
Завдання рольового керування доступом з обмеженням (деякі операції (їх підмножина) несумісні для всіх ролей)

Для моделі узагальненої RBAC системи:
-Напішіте модель системи за умови, що активні ролі системи не можуть одночасно включати деякий дозвіл p
-Опішіть зміну поточного стану системи за умови видалення дозволу t
-Напішіть модель системи за умови, що ролі r1 і r2 виключають одна одну для деякого користувача.

Література:

Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие. – Екатеринбург: 2008, 212 с. [с. 112-132, 181-189]

Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М. Изд. центр “Академия”, 2005 – 144 с. [с. 88-101]

Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. – М.: Феникс, 2008 - 178 с. - ISBN 978-5-222-13164-0 [с. 47-49]

Корт С.С. Теоретические основы защиты информации. Учебное пособие для вузов. - М. Гелиос АРВ, 2004 — 240 с. ISBN: 5-85438-010-2 [гл.8]