УДК 004.056.55

Волинець С.Ю.

Салієва О.В.

АНАЛІЗ ВПРОВАДЖЕННЯ ДИНАМІЧНИХ РОЛЕЙ У КОНТЕКСТІ РОЛЬОВОЇ ПОЛІТИКИ РОЗМЕЖУВАННЯ ДОСТУПУ

Вінницький національний технічний університет

Анотація

В даній роботі розглянуто ідею впровадження динамічних ролей у класичну рольову політику розмежування доступу для підвищення рівня захищеності інформації. Запропоновано методи їх реалізації. Проведено порівняння статичних та динамічних ролей.

Ключові слова: Рольова політика безпеки, керування доступом на основі ролей, динамічні ролі.

Abstract

This paper discusses an idea of implementing dynamic security roles into a classic role-based access control to improve information security. Methods of their implementation are proposed. Static and dynamic security roles are compared.

Keywords: Role-based security policy, role-based access control, dynamic security roles.

Вступ

Зазвичай, рольова політика розмежування доступу ґрунтується на статичних ролях, які залишаються незмінними. Однак, використання динамічних ролей, які можуть змінюватися залежно від контексту, забезпечує більш гнучкий та адаптивний контроль доступу. Розгляд такої концепції є особливо актуальним сьогодні, адже стрімкий розвиток інформаційних технологій зумовлює зростання потреб у їх захищеності та безпеці конфіденційних даних.

Результати дослідження

Рольова модель контролю доступу (RBAC) – це метод керування доступом до ресурсів в інформаційних системах, який використовує ролі для визначення прав користувачів. При чому, роль – це набір дозволів, що описують дії, які користувач може виконувати з певними ресурсами. RBAC здобула широку популярність завдяки своїй простоті та гнучкості. Її легко зрозуміти та адмініструвати, а також вона може бути легко адаптована до різних типів інформаційних систем [1].

Розглянемо переваги рольової моделі контролю доступу [2]:

– простота використання. RBAC легко зрозуміти, адже користувачу не потрібно знати про складні дозволи та правила, йому достатньо знати свою роль;

– легкість впровадження. Модель може бути легко адаптована до різних типів інформаційних систем. Ролі можна легко створити, змінити та видалити;

– масштабованість. Рольова політика може бути легко масштабована для підтримки великої кількості користувачів і ресурсів;

– безпека. RBAC може допомогти покращити безпеку інформаційних систем, надаючи доступ до ресурсів лише тим користувачам, які його потребують;

– зручність. Впровадження рольової моделі забезпечує зручність для користувачів, адже їм не потрібно вручну запитувати доступ до ресурсів.

Проте рольова модель контролю доступу має певні недоліки [3]:

– жорсткість. RBAC може бути жорсткою моделлю, адже вона не завжди може врахувати всі нюанси доступу до ресурсів;

– складність адміністрування. Адміністрування може бути складним завданням, адже адміністраторам потрібно знати про всі ролі та дозволи в системі, незважаючи на велику кількість різноманітних або аналогічних ролей, які мають відмінності;

– необхідність оновлення. RBAC може потребувати регулярного оновлення, адже ролі та дозволи можуть часто змінюватися з часом;

– небезпека зловживання. RBAC може бути використана для зловживання, адже користувачі з високими привілеями можуть отримати доступ до ресурсів, до яких вони не повинні мати доступ.

Проаналізувавши загальні положення, переваги та недоліки рольової моделі контролю доступу та тенденцію розвитку сучасних технологій, варто розглянути можливість додавання до RBAC динамічних ролей.

Динамічна роль – це роль, яка присвоюється користувачеві на основі динамічних атрибутів користувача та середовища. Ці атрибути можуть включати місцезнаходження користувача, тип пристрою, час доби, історію дій користувача, поточний стан системи та інші [4].

Перевагами використання динамічних ролей є те, що на відміну від статичних ролей вони:

– адаптуються. Динамічні ролі можуть адаптуватися до мінливих потреб користувачів та середовища;

– гнучкі. Вони є зручним інструментом для покриття потреби у ручному оновленні конкретних дозволів;

– деталізовані. Динамічні ролі можуть врахувати всі нюанси доступу до ресурсів, такі як обмеження пов’язані із часом доби або місцезнаходженням, що робить їх більш точними;

– Ефективні. Динамічні ролі економлять час та ресурси, адже вони не потребують ручного оновлення;

– спрощують адміністрування. Адміністрування динамічних ролей може бути простішим, адже система автоматично оновлює ролі.

Відобразимо загальні відмінності між статичними та динамічними ролями у таблиці 1.

Таблиця 1 – Відмінності між статичними та динамічними ролями

Критерій	Статичні ролі	Динамічні ролі
Процес оновлення	Оновлюються адміністратором вручну	Оновлюються автоматично на основі динамічних атрибутів
Ефективність	Потребують більшого часу та ресурсів за рахунок ручного оновлення	Економлять час та ресурси
Деталізація	Не завжди враховують всі нюанси доступу	Можуть врахувати всі нюанси доступу
Адміністрування	Складні для адміністрування	Спрощують адміністрування
Адаптивність	Не адаптивні	Адаптуються до мінливих потреб
Безпека	Мають певні ризики зловживання	Ризик зловживання знижений за рахунок адаптації
Розуміння	Легко зрозуміти та реалізувати	Можуть виникнути складнощі у розумінні та процесі реалізації

Таким чином, для більшості критеріїв відображених в таблиці 1, динамічні ролі можуть бути кращим рішенням, аніж статичні, але їх розуміння та процес реалізації може бути важчим для відповідних спеціалістів.

Розглянемо методи реалізації концепції динамічних ролей [4]:

– атрибутна модель. Ролі генеруються на основі динамічних атрибутів користувача та середовища;

– політики доступу. Правила доступу динамічно визначаються на основі контексту;

– машинне навчання. Алгоритми машинного навчання використовуються для прогнозування необхідних дозволів;

– комбінований підхід. Використання декількох методів для забезпечення більшої гнучкості та точності.

В залежності від вимог до рівня захищеності інформації в інформаційній системі можна обрати один або кілька із запропонованих методів.

Проаналізувавши рольову модель контролю доступу, можна зазначити, що динамічні ролі – це перспективний метод керування доступом, який може допомогти покращити безпеку, адміністрування та ефективність інформаційних систем.

Висновок

Підбиваючи підсумки проведеного дослідження, зазначимо, що сама по собі рольова модель контролю доступу є популярною та самодостатньою. Вона добре піддається масштабуванню та водночас є зручною і безпечною. Для розширення моделі та покращення її точності й ефективності було розглянуто ідею впровадження динамічних ролей. Такі ролі можуть значно покращити рівень захищеності інформації за рахунок полегшення адміністрування та автоматичної зміни ролі в залежності від мінливих потреб та контексту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Role-Based Access Control [Електронний ресурс] / Official Documentation // auth0.com – 2024 – Режим доступу до ресурсу: https://auth0.com/docs/manage-users/access-control/rbac
2. Role-based access control (RBAC) [Електронний ресурс] / Alexander S. Gillis // techtarget.com – 2023 – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/role-based-access-control-RBAC
3. What is RBAC? (Role Based Access Control) [Електронний ресурс] / Digital Guide // Ionos, – 2023. – Режим доступу до ресурсу: https://www.ionos.com/digitalguide/server/security/what-is-role-based-access-control-rbac/
4. The Case for Dynamic Role-based Access Control [Електронний ресурс] / Dane Stuckel // softwarepatterns.com – 2022. – Режим доступу до ресурсу: https://softwarepatterns.com/articles/dynamic-role-based-access-control/

Волинець Сергій Юрійович – студент групи 2КІТС-20б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: datynford@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Volynets Serhii Y. – student of 2KITS-20b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: datynford@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@gmail.com