УДК 004.056.55

А. В. Приймак
О. В. Салієва

ВДОСКОНАЛЕННЯ МОДЕЛІ RBAC У ПРИВАТНИХ ХМАРНИХ СЕРЕДОВИЩАХ

Вінницький національний технічний університет

Анотація

В результаті проведеної роботи було розроблено гібридну модель авторизації на основі виразів та RBAC, яка складається з 9 кроків і динамічно дає рішення про доступ до ресурсу чи операції, в залежності від поточного налаштування. Порівняння запропонованої модифікації з існуючими показало, що розроблена модель має вищий коефіцєнт правильності надання доступу користувачеві в середньому на 1,5–11,5%.

Ключові слова: захист інформації, приватні хмарні середовища, моделі керування доступом, ролі.

Abstract

As a result of the work, a hybrid model of expression-based authorization and RBAC was developed, consisting of 9 steps and dynamically deciding access to a resource or operation, depending on the current configuration. Comparison of the proposed modification with the existing ones showed that the developed model has a higher coefficient of correctness of granting access to the user by an average of 1.5-11.5%.

Keywords: information security, private cloud environments, access control models, roles.

Вступ

В даний час все більшої популярності набувають хмарні технології. Це пов’язано з стрімким розвитком Інтернету і супутніх технологій. На багатьох підприємствах люди працюють у віддаленому режимі, передаючи всю необхідну інформацію через інтернет [1]. Хмарні технології надають споживачам рішення, повністю готові до роботи. Достатньо володіти будь-яким пристроєм, здатним з’єднатися з інтернетом, і можна отримати доступ до віддаленої бази, яка розташовується на віддаленому сервері. Крім того, користувачеві хмарних сервісів не потрібно піклуватися про інфраструктуру, яка забезпечує працездатність сервісів, що надаються йому. Усі завдання по налаштуванню, усуненню несправностей, розширенню інфраструктури та інших бере на себе сервіс-провайдер [2]. Проаналізувавши існуючі модифікації моделі RBAC, стало зрозуміло, що правильність надання доступу знаходиться в межах від 72% до 96%, крім того, також можна виділити такі недоліки, як мала гнучкість налаштування, необхідність попереднього визначення політики доступу та при її модифікації необхідність модифікації самого продукту, а тому залишається актуальним підвищення даного коефіцієнту і розробки відповідної моделі, яка усуне вищеперераховані недоліки.

Результати дослідження

Запропонована модель авторизації складається з таких кроків:

1. Початок процедури авторизації користувача в системі.
2. Отримання виразів для певного користувача (попередньо внесеними до системи адміністратором).
3. Перевірка виразу.
4. У разі виконання виразу, система перевіряє інші вирази, після чого формується рішення щодо надання доступу.
5. У разі невиконання якогось з виразів, система одразу формує негативне рішення щодо надання доступу користувачу, без подальшої перевірки виразів.

Додаток з використанням моделі авторизації на основі виразів буде повністю захищеним, оскільки при відсутності даних, необхідних для проходження виразу (умови), запит на ресурс чи операцію буде відхилено.

Схема роботи моделі авторизації на основі виразів представлена на рисунку 1.

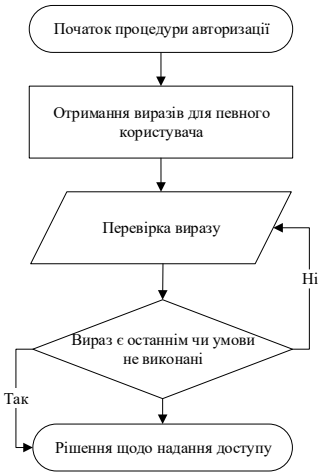

Рисунок 1 – Схема роботи моделі авторизації на основі виразів

Запропонована модель авторизації на основі виразів показала високі результати правильності надання доступу (92-97%), що показує високу точність та надійність її роботи. Порівняльна характеристика існуючих модифікацій моделі RBAC з запропонованою моделлю показала, що запропонована модель показала вищі показники в середньому на 11% ніж модель MT-RBAC, на 7.5% вищі ніж CAACM, на 11,5% вищі ніж GEO-RBAC, а також на 1.5% та 8% вищі ніж моделі SAT-RBAC і ABAC відповідно.

Висновки

Було запропоновано гібридну модель авторизації на основі виразів та RBAC, яка складається з 9 кроків і динамічно дає рішення про доступ до ресурсу чи операції, в залежності від поточного налаштування. Гнучкість була досягнута шляхом використання виразів, які можна змінити під час експлуатації додатку. В свою чергу об'єднання з RBAC додало простоту модифікації під час застосування, оскільки для виконання певної операції користувач має мати роль, якій відповідають певні вирази, тобто роль може змінювати своє значення під час роботи додатку, без необхідності зміни програмного коду.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Данилюк І.І., Карпінець В.В., Приймак А.В., Яремчук Ю.Є., Костюченко О.І. Метод ідентифікації користувача за клавіатурним почерком на основі нейромереж. Реєстрація, зберігання і обробка даних, Т. 20, №2, 2018. С. 68–76.

2. Sedighi A., Jacobson D. Forensic Analysis of Cloud Virtual Environments. *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC).* New York, USA. – 2019, P. – 323-329.

Приймак Андрій Васильович — аспірант, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: andrii.pryimak@live.com.

Салієва Ольга Володимирівна — аспірант, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com.

Науковий керівник: ***Яремчук Юрій Євгенович*** — доктор технічних наук, професор, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.

Pryimak Andrii Vasyliovych — postgraduate, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: andrii.pryimak@live.com.

Salieva Olha Volodymyrivna— postgraduate, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: salieva8257@gmail.com.

Supervisor: ***Yaremchuk Yuriy E***. — D. Sc., professor, management and security of information Systems department; Vinnitsa.