УДК 005.311.6:519.86

ПРОБЛЕМА ПРИЙНЯТТЯ РІШЕНЬ У ГІБРИДНИХ МОДЕЛЯХ АВТОРИЗАЦІЇ ДЛЯ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Василенко О.В.
e-mail: ostap.vasylenko@nure.ua
Науковий керівник – канд. техн. наук, доц. Матвієнко О.І.
Харківський національний університет радіоелектроніки,
кафедра прикладної математики
м. Харків, Україна

Modern distributed information systems are characterized by such features as a large number of users and services, geographical distribution of components, dynamic access policies, and different levels of trust in system nodes. In this work, a model for access decision-making in a hybrid authorization system is proposed, based on the verification of user roles, the analysis of user and resource attributes, and the assessment of contextual access risk.

Сучасні розподілені інформаційні системи (Distributed Information Systems) характеризуються такими особливостями, як велика кількість користувачів і сервісів, географічна розподіленість компонентів, динамічні політики доступу, різні рівні довіри до вузлів системи тощо. У таких системах класичні механізми контролю доступу часто не забезпечують достатньої гнучкості та масштабованості. Отже, актуальною є проблема прийняття рішень у гібридних моделях авторизації для розподілених інформаційних систем в умовах сучасних мережевих середовищ, хмарних сервісів та мікросервісної архітектури. Мікросервісні архітектури та хмарні платформи створюють тисячі взаємодій між компонентами, рішення про доступ часто залежить від ролі користувача, атрибутів, контексту (час, місце, пристрій), історії поведінки, а атаки типу privilege escalation, lateral movement вимагають більш інтелектуальних механізмів авторизації.

Найбільш поширеними є наступні моделі: RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control), DAC (Discretionary Access Control) та MAC (Mandatory Access Control). Так, наприклад, у моделі RBAC доступ визначається роллю користувача, а у моделі ABAC – атрибутами суб’єктів, об’єктів та контексту. На практиці виникає потреба гібридних моделей, що поєднують кілька підходів. Гібридні моделі поєднують RBAC і ABAC, RBAC і контекстні політики, ABAC і машинне навчання. Такі моделі використовуються у хмарних системах, Zero Trust архітектурі, розподілених API-шлюзах тощо. Велику частину сучасних досліджень спрямовано на підвищення інтелектуальності та адаптивності систем авторизації [1].

Розглянемо узагальнену модель гібридної авторизації. Позначимо множини U – множину користувачів (суб’єктів доступу), O – множину об’єктів доступу, A – множину можливих дій над об’єктами (read, write, execute), R – множину ролей, C – множину можливих контекстів доступу. Запит

доступу описується четвіркою $q=(u,o,a,c)$, де $u\in U$ – користувач, $o\in O$ – об'єкт, $a\in A$ – дія, $c\in C$ – контекст. Для гібридної моделі авторизації вводяться вектори атрибутів: атрибути суб'єкта $S(u)=(s_1,s_2,...,s_n)$, де s_i – i-й атрибут користувача, (роль, рівень доступу, організаційна приналежність тощо), $i=1,\ 2,\ ...,\ n$, атрибути об'єкта $T(o)=(t_1,t_2,...,t_m)$, де t_j – j-й атрибут ресурсу (клас конфіденційності, тип ресурсу, критичність), $j=1,\ 2,\ ...,\ m$, атрибути середовища $E(c)=(e_1,e_2,...,e_k)$, де e_l – l-й параметр контексту (час доступу, IP-адреса, тип пристрою, мережеве середовище), $l=1,\ 2,\ ...,\ k$.

Процедура прийняття рішення задається функцією

$$D:U\times O\times A\times C\to\{0,\ 1\},$$

де $D=1$, якщо доступ дозволено, і $D=0$, якщо доступ заборонено.

У гібридній моделі рішення формується на основі трьох компонентів: рольова модель (RBAC), атрибутна модель (ABAC) і контекстна оцінка ризику. Для RBAC-компоненти функція перевірки ролей має вигляд

$$F_{RBAC}(u,a)=\begin{cases}1, & (role(u),\ a)\in PA,\\ 0, & (role(u),\ a)\notin PA,\end{cases}$$

де $role(u)$ – роль користувача, $PA\subseteq R\times A$ – відношення призначення прав ролям. Для ABAC-компоненти атрибутна перевірка описується функцією

$$F_{ABAC}(u,o)=g(S(u),\ T(o)),$$

де $g(\cdot,\ \cdot)$ – політика доступу, що аналізує атрибути суб'єкта та об'єкта. Контекстний ризик визначається функцією

$$Risk=h(E(c)),$$

де $h(\cdot)$ – функція оцінки ризику доступу.

Фінальне рішення системи визначається правилом

$$D(u,o,a,c)=\begin{cases}1, & F_{RBAC}(u,a)=1\wedge F_{ABAC}(u,o)=1\wedge Risk<R_{crit},\\ 0, & \text{інакше,}\end{cases}$$

де R_{crit} – гранично допустимий рівень ризику.

Отже, рішення про доступ у гібридній системі авторизації пропонується формувати шляхом перевірки ролей користувача, аналізу атрибутів користувача і ресурсу та оцінки контекстного ризику доступу. Доступ надається лише тоді, коли всі компоненти моделі задовольняють політику безпеки.

Список використаних джерел:

1. Penelova M. Hybrid Role and Attribute Based Access Control Applied in Information Systems. Cybernetics and Information Technologies. 2021. Vol. 21, No. 3. P. 85-96. DOI: 10.2478/cait-2021-0031.