УДК 004.056

Орлова Ю.Ю.

АНАЛІЗ МОДЕЛЕЙ РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

Вінницький національний технічний університет

Анотація
Метою даної роботи є аналіз моделей розмежування прав доступу до інформаційних ресурсів.
Ключовіслова:модель, інформаційні ресурси.

Abstract
The purpose of this work is to analyze the models of delimitation of access rights to information resources.
Keywords:model, information resources.

Вступ

Сьогодні ми можемо спостерігати бурхливий розвиток інформаційних технологій. Обчислювальна техніка стає застарілою лише за декілька років, а її технічні характеристики ростуть експоненційно. З розвитком цих технологій все більше різних компаній використовують інформаційні технології для автоматизації їх бізнесу. Ці зміни суттєво збільшують обсяги важливої інформації, що зберігаються у центрах обробки даних та хмарних сховищах , що призведе до збільшення навантаження на такі сховища. Це формулює тенденцію використовувати розподілені системи даних все більше.Багато з таких існуючих систем мають проблеми с розмежуванням доступу. У даній роботі буде розглянуто використання різних моделей розмежування доступу до інформаційних ресурсів.

Основна частина

Розмежування доступу — сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі правил розмежування доступу [1].

Правила розмежування доступу — частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об’єктів [1].

При розгляді взаємодії двох об'єктів комп’ютерної системи, що виступають як приймальники або джерела інформації, слід виділити пасивний об'єкт, над яким виконується операція, і активний об'єкт, який виконує або ініціює цю операцію[2]. Коли користувачі або процеси намагаються одержати доступ до пасивних об'єктів, механізми, що реалізують керування доступом, на підставі політики безпеки і перевірки атрибутів доступу можуть «прийняти рішення» про легальність запиту. Використовуючи набір атрибутів доступу відповідно до прийнятої політики безпеки, можна реалізувати потрібне керування доступом.

Дискреційні методи розмежування доступу[3].

Дана модель характеризується розмежуванням доступу між названими суб'єктами та об'єктами. Суб'єкт з певним правом доступу може передавати це право будь-якому іншому суб'єкту. Для кожної пари (суб'єкт - об'єкт) повинно бути задано явне і недвозначне перерахування допустимих типів доступу (читання,писання тощо), які є санкціонованими для даного суб'єкта до даного ресурсу. Кожен об'єкт системи має прив'язаний до нього суб'єкт, що називається власником. Власник встановлює права доступу до об'єкта. Система має єдиний виділенний привілейований суб'єкт, який уповноважений встановлювати права власності для всіх інших суб'єктів системи. Можливо і змішані варіанти побудови, коли одночасно в системі присутні як власники, встановлюючи права доступу до своїх об'єктів, так і привілейовані субє’кти, що мають можливість змінити права для будь-якого об'єкта, або зміни його власника. Такий змішаний варіант реалізується в більшості операційних систем. Дискреційне керування доступом є основною реалізацією розмеженої політики доступу до ресурсів при обробці конфіденційних відомостей відовідно до вимог до системи захисту інформації. Основний елемент дискреційного розмежування доступу є матриця доступу.

Мандатні методи розмежування доступу[4].

Для реалізації цього принципу кожному суб'єкту і об'єкту повинні скласти класифікаційні мітки, що відображають місце даного суб'єкта (об'єкта) у відповідній ієрархії. За допомогою цих міток

суб'єктам і об'єктам повинні призначатися класифікаційні рівні (рівні уразливості, категорії секретності), які є комбінаціями ієрархічних і неієрархічних категорій. Дані мітки повинні служити основою мандатної принципу розмежування доступу. Комплекс засобів захисту (КСЗ) при введенні нових даних в систему повинен запитувати і отримувати від санкціонованого користувача класифікаційні мітки цих даних. При санкціонованому занесенні в список користувачів нового суб'єкта має здійснюватися зіставлення йому класифікаційних міток. КСЗ повинен реалізовувати мандатний принцип контролю доступу стосовно до всіх об'єктів при явному і прихованому доступі з боку будь-якого із суб'єктів. Суб'єкт може читати об'єкт, тільки якщо ієрархічна класифікація суб'єктом не менше, ніж ієрархічна класифікація об'єкта, і якщо не ієрархічні категорії суб'єкта включають в себе всі ієрархічні категорії об'єкта. Суб'єкт здійснює запис в об'єкт, тільки якщо класифікаційний рівень суб'єкта максимум, ніж класифікаційний рівень об'єкта, і всі ієрархічні категорії суб'єкта включаються в неієрархічні категорії об'єкта. Реалізація мандатних правил розмежування доступу повинна передбачати можливості супроводу зміни класифікаційних рівнів суб'єктів і об'єктів спеціально виділеними суб'єктами [5]. Повинен бути реалізований механізм доступу, що здійснює перехоплення всіх звернень суб'єктів до об'єктів, а також розмежування доступу відповідно до заданого принципом розмежування доступу.

В організаціях з різнорідною IT-інфраструктурою, що містять десятки і сотні систем і додатків, допомагає використання ієрархії ролей і успадкування привілеїв. Без цього використання рольової моделі стає вкрай заплутаним. Для великих систем з сотнями ролей, тисячами користувачів і мільйонами дозволів, управління ролями, користувачами, дозволами і їх взаємозв'язками є складним завданням, яке неможливо здійснити малою групою адміністраторів безпеки [6]. Привабливою можливістю є використання самої рольової моделі для сприяння децентралізованому управлінню ролями. Рольова модель широко використовується для управління призначеними для користувача привілеями в межах єдиної системи або єдиного додатку.

Висновки

Уданій роботі було проаналізовано дискреційну і мандатну модель доступу до інформаційних ресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Розмежування доступу [Електронний ресурс] –Режим доступу до ресурсу: https://studfile.net/preview/5206326/page:7/
2. Основи управління інформаційною безпекою[Електронний ресурс] –Режим доступу до ресурсу: https://studopedia.org/12-73925.html
3. Рольова модель[Електронний ресурс] –Режим доступу до ресурсу:https://csrc.nist.gov/projects/role-based-access-control/faqs
4. Моделі та методи контролю доступу[Електронний ресурс] –Режим доступу до ресурсу: https://worldvision.com.ua/ua/modeli-i-metody-kontrolya-dostupa-chto-vam-podkhodit/
5. Розробка моделей прав доступу [Електронний ресурс] –Режим доступу до ресурсу: https://cyberleninka.ru/article/n/razrabotka-modeli-razgranicheniya-prav-dostupa-dlya-avtomatizirovannyh-sistem-tehnologicheskogo-upravleniya
6. Підходи до контролю доступа [Електронний ресурс] –Режим доступу до ресурсу: https://habr.com/ru/company/custis/blog/248649/

Орлова Юлія Юріївна— студент групи 2бс-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Дудатьєв Андрій Веніамінович*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця.

Orlova Yuliya Y. — student of group 2bs-17b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia

Supervisor: ***Dudatyev Andriy V.*** — Cand. Sc. (Eng), Assistant Professor of information protection, Vinnytsia National Technical University, Vinnytsia