УДК 004.056

Ю. В. Баришев
К. В. Неуйміна

МЕТОД РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ З ПРИВ'ЯЗКОЮ ДО РОБОЧОЇ СТАНЦІЇ

Вінницький національний технічний університет

Анотація

В даній роботі представлено аналіз моделей розмежування прав доступу. Запропоновано метод розмежування доступу, що використовуючи особливості процесу гешування дозволяє обмежити перелік робочих станції, з яких користувачу дозволяється отримувати віддалений доступ до інформаційних ресурсів.

Ключові слова: автентифікація, гешування, пароль, модель розмежування прав доступу, параметри робочої станції.

Abstract

Access control models analyses are performed at the work. The access control method which uses hashing peculiarities allows to limit the workstations quantity from which users are allowed to get remote access to information resources.

Keywords: authentication, hashing, password, access control model, workstation parameters.

Вступ

Внаслідок наявності багатьох можливих джерел порушення безпеки інформації, що обробляється з використанням засобів обчислювальної техніки [1-3], виникає задача забезпечення захищеності цієї інформації без істотного погіршення показників якості реалізації процесу обробки цієї інформації. Одним з методів захисту, які використовуються для розв'язання цієї задачі, є розмежування доступу користувачів комп'ютерної системи до наявних в системі інформаційних ресурсів [2, 3].

Метою даного дослідження є покращення захищеності конфіденційності інформації, що віддалено надається користувачам інформаційної системи.

Для досягнення мети необхідно розв'язати низку задач. Дана робота направлена на розв'язання таких з них:

- аналіз моделей розмежування прав доступу щодо можливості їх використання для досягнення мети дослідження;
- розробка методу автентифікації користувачів, який дозволяє реалізовувати обрану модель розмежування прав доступу.

Моделі розмежування прав доступу

Під час дослідження аналізувались такі моделі: модель Харрісона-Руззо-Ульмана, яка передбачає представлення системи розмежування прав доступу кінцевим автоматом; модель Take-Grant – основним завданням моделі є визначення можливості одержання прав доступу суб'єктом системи на об'єкт у стані, описаному графом доступів, модель Белла-ЛаПадула – за грифами секретності розподіляються об'єкти, наявні в інформаційній системі, та за рівнями секретності (мандатами) суб'єкти, що діють в цій системі, базова модель рольового розмежування прав доступу [1-3].

Загальним недоліком даних моделей є те, що вони не забезпечують обмеження робочих станцій, з яких користувач має право отримувати доступ. Останній недолік стає значущим в системах надання доступу до розподілених інформаційних ресурсів, зокрема файлових серверів та хмарних сервісів

Для даного дослідження обрано модель розмежування прав доступу, що пропонується в статті [4]. Дана модель передбачає формування правил надання доступу залежно від автентифікаційних даних користувача та робочих станцій з використанням яких користувачу дозволено отримувати доступ до певного інформаційного ресурсу.

Метод автентифікації користувачів

Реалізація обраної моделі розмежування прав доступу вимагає розробки методу автентифікації користувачів. Відповідно пропонується метод, що виконується відповідно до схеми наведеної на рис. 1.

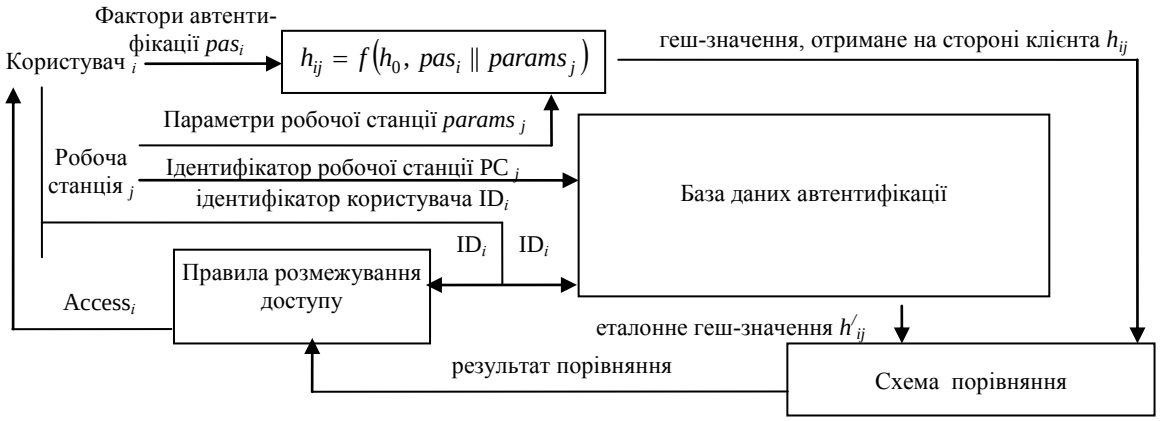

Рис. 1. Схема автентифікації

База даних автентифікації, на ведена на рис. 1, містить ідентифікатор користувача, геш-значення факторів автентифікації користувачів, набір прав доступу для користувачів, ідентифікатори робочих станцій. Як видно з рис. 1 даний метод, використовуючи ітеративність конструкції гешування дозволяє використовувати геш-значення факторів автентифікації користувачів як ключ гешування параметрів робочої станції. На основі методу розроблено схему системи автентифікації, що реалізує надання доступу до розподілених інформаційних ресурсів. На стороні клієнта відбувається гешування факторів автентифікації користувача та параметрів робочої станції. На стороні сервера відбувається гешування параметрів робочої станції, з якою користувачеві дозволено працювати, використовуючи геш-значення як ключ гешування. Якщо геш-значення збігаються, автентифікація вважається успішною, якщо ж ні – надсилається запит на отримання параметрів наступної робочої станції, з якою користувачеві дозволено працювати, з їх подальшим гешуванням.

Висновки

Відповідно до проведеного аналізу моделей розмежування прав доступу, визначено, що існує низка задач, для яких важливо обмежити перелік робочих станцій, з яких користувач може отримувати доступ до критичних інформаційних ресурсів. За результатами цього аналізу визначено модель, що дозволяє забезпечити обмеження робочих станцій, з яких користувач має право отримувати доступ. Для реалізації обраної моделі запропоновано метод автентифікації користувачів та структуру системи розмежування прав доступу, які за рахунок ітеративності процесу гешування дозволили виконати прив'язку користувачів до робочих станцій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Девянин П.Н. Модели безопасности компьютерных систем / П. Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.

2. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / [А. А. Афанасьев и др.]; Под ред. А. А. Шелупанова, С. Л. Груздева. – М.: Горячая линия – Телеком, 2009. – 552 с.

3. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця: ВНТУ, 2013. – 221 с.

4. Баришев Ю. В. Метод автентифікації віддалених користувачів для мережевих сервісів / Ю. В. Баришев, В. А. Каплун // Інформаційні технологій та комп'ютерна інженерія. – 2014.– №2. – С. 13-17.

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна, yuriy.baryshev@gmail.com

Неуйміна Крістіна Володимирівна – студентка, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна, kris.vladimirovna99@gmail.com

Yurii Baryshev – Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, yuriy.baryshev@gmail.com

Kristina Neuimina – Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, kris.vladimirovna99@gmail.com.