УДК 004.056.53(043.2)

Луцько П.В.
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ ПРОТОКОЛУ KERBEROS ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПІД ЧАС РОБОТИ З РЕСУРСАМИ ЛОКАЛЬНОЇ МЕРЕЖІ

Розвиток мережевих технологій, вдосконалення програмного і апаратного забезпечення, а разом з цим і виникнення нових підходів до використання комп'ютерних мереж призвели до стрімкого збільшення їх кількості. Поширена в сфері IT концепція інтеграції персональних комп'ютерів та різноманітного офісного та побутового обладнання, а також розширення переліку доступних в локальній мережі послуг призвели до появи необхідності автентифікації користувачів під час роботи з ресурсами локальної мережі.

Одним з методів автентифікації користувачів в локальній мережі є мережевий проткол Kerberos, що передбачає механізм взаємної автентифікації в умовах незахищеного каналу зв'язку. Інтеграція протоколу Kerberos в процес обміну даними в локальній мережі дозволяє підвищити рівень захисту інформації від несанкціонованого доступу. Процес автентифікації відбувається шляхом обміну повідомленнями встановленого формату між клієнтським програмним забезпеченням та центром розповсюдження ключів (KDC), де зберігається інформація про користувачів та доступні їм ресурси локальної мережі.

Зважаючи на характерну для локальних мереж різнорідність програмних продуктів, що приймають участь у взаємодії між вузлами доцільно, серед можливих варіантів програмної реалізації протоколу Kerberos, обрати дворівневу (клієнт-сервер) архітектуру програмної системи. Клієнтське програмне забезпечення даної системи реалізується у вигляді proxy-серверу, що приймає участь в процесі автентифікації від імені користувача чи серверу-послуг, до безпосереднього використання користувачем мережевої послуги. Серверне програмне забезпечення виконує функції KDC і представляє собою програмний додаток котрий приймає запити від клієнтів та виконує їх перевірку на основі інформації про користувачів та послуги мережі. З метою організації збереження та обробки даних, що використовуються в процесі автентифікації в структуру серверного програмного забезпечення входить реляційна база даних.

Запропонована концепція реалізації протоколу Kerberos в локальній мережі дозволяє проводити процес автентифікації незважаючи на особливості реалізації програмного продукту, що забезпечує конкретну мережеву послугу. До переваг також можна віднести наявність незалежного від платформи формату повідомлень, що дозволяє взаємодію вузлів під керуванням операційних систем різних видів.

Необхідно відмітити, що описане рішення має певні очевидні недоліки. Так можлива ситуація, коли витрати часу на процес автентифікації можуть створювати помітну для користувача затримку відповіді серверу послуг. Також протокол Kerberos вимагає використання одного з вузлів мережі в ролі KDC. Окрім перелічених недоліків існує необхідність у заповненні та підтримці в актуальному стані користувачем бази даних облікових записів.

Науковий керівник – Н.І. Алішов, д.т.н.,проф.