УДК 004.056

ВІДДАЛЕНА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ QR-КОДУ

О. П. Войтович, к.т.н., доц., Р. О. Коломієць
Вінницький національний технічний університет
o_p_v@list.ru

Однією з основних задач систем захисту від несанкціонованого доступу до інформаційно-комунікаційних систем є автентифікація. Автентифікація користувачів є однією з базових процедур для забезпечення безпечного зв'язку та обміну даними по незахищеному каналу відкритих мереж. Таким чином, простий і ефективний механізм перевірки автентичності є необхідним для забезпечення мережевої безпеки в реальному навколишньому середовищі. Загалом, механізм парольної автентифікації забезпечує основні можливості для запобігання несанкціонованому доступу. Досить ефективними є методи автентифікації на основі одноразових паролів, які дозволяють знизити ризики фальсифікації і витрати на технічне обслуговування. Проте більшість методів мають певні обмеження, зазвичай пов’язані з технічною складовою, або ускладненням роботи користувача.

Досить цікавим методом формування одноразових паролів є метод з використанням мобільних технологій. На сьогоднішній день майже всі користувачі Інтернету мають мобільні телефони, які в свою чергу мають достатньо ресурсів для використання QR-кодів.

QR-код (англ. quick response — швидкий відгук) – це двовимірний штрих-код, який несе в собі інформацію, яку може зчитувати користувач за допомогою пристрою з вбудованою камерою. Завдяки легкому розпізнаванню абонент може швидко занести в свій пристрій текстову інформацію, за допомогою якої отримує відповідні послуги(додавати контакти в телефону книгу, переходити по web, відправляти повідомлення та ін.).

Пропонована схема автентифікації включає в себе дві сторони: сервера (Server) і віддалених користувачів, кожен авторизований користувач може запросити обслуговування від Server на надання прав доступу. Крім того, кожному користувачу необхідно мати мобільний телефон із встановленим спеціальним програмним забезпеченням. Також телефон повинен містити вбудовану камеру, щоб зняти зображення QR-коду і потім розшифрувати його.

Раніше запропонована схема автентифікації здійснюється у два етапи і вимагає більше часу та ресурсів як зі сторони користувача, так і зі сторони сервера, хоча і забезпечує більш стійкий захист сторін. Якщо вимоги забезпечення безпеки не є критичними, то більш доцільним є використання спрощеної схеми.

Спрощена схема автентифікації здійснюється таким чином (рис.1):

1) Користувач А на мобільному пристрої в спеціальному встановленому програмному засобі вводить логін та пароль, значення гешуються і відправляються на Server.

2) Server генерує і виводить геш-значення на основі коду URL(зашифрованого) у вигляді QR-коду.

3) Користувач А за допомогою мобільного пристрою сканує QR-код. До отриманих значень додається LP h(LP+QR-код).

4) Якщо все було виконано вірно – надається доступ, в іншому випадку запит відхиляється.

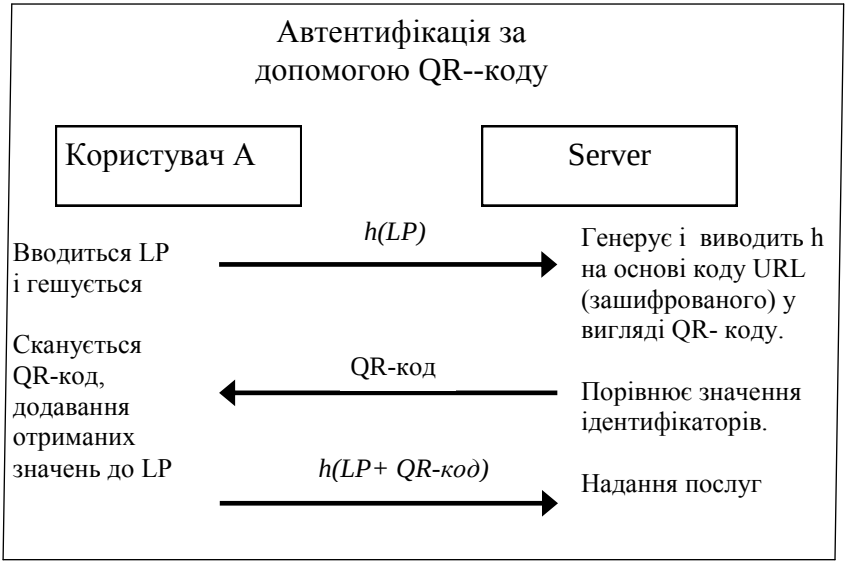

Рисунок 1 – Схема автентифікації

h() – геш-функція на основі коду, що використовує URL;
LP – логін та пароль.

Механізм автентифікації за допомогою QR-коду забезпечує основні можливості для запобігання від несанкціонованого доступу.

Отже запропоновано для автентифікації віддалених користувачів використовувати технологію одноразових паролів на основі QR-кодів, що не тільки усуває використання таблиці перевірки пароля, але і є економічно ефективним рішенням, так як більшість користувачів Інтернету вже мають мобільні телефони.