УДК 004.056

В. І. Селезньов

МОДУЛЬ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Вінницький національний технічний університет;

Анотація

Проаналізовано відомі методи автентифікації. Розглянуто важливість використання стійкого алгоритму автентифікації користувачів у серверних застосунках. Розроблено модуль автентифікації користувачів, що дозволяє підвищити стійкість односторонньої автентифікації на серверному застосунку.

Ключові слова: автентифікація користувача, криптографічний протокол, алгоритм, доведення з нульовим знанням.

Abstract

The analysis of known authentication methods was performed. The importance of using a stable algorithm for user authentication in server applications is considered. An authentication module has been developed, which allows to increase the stability of one-sided authentication on a server application.

Keywords: user authentication, cryptographic protocol, algorithm, zero knowledge proof.

Вступ

Автентифікація – це процедура перевірки справжності суб'єкта, яка дозволяє достовірно переконатись у тому, що суб'єкт, який пред'явив свій ідентифікатор, насправді є саме тим суб'єктом, ідентифікатор якого він використовує [1].

На сьогоднішній день, засоби автентифікації користувачів не завжди дозволяють забезпечити достатній рівень стійкості, оскільки в основі використовують протоколи, побудовані на основі відомих шифрів, геш-функцій, обчислень певних математичних задач тощо. Тому створення модуля автентифікації на основі модифікованого протоколу автентифікації є актуальним на сьогодні [2].

Метою дослідження є підвищення стійкості автентифікації користувачів на серверних застосунках.

Для досягнення мети необхідно:

- проаналізувати відомі протоколи автентифікації;
- розробити протокол автентифікації користувачів;
- реалізувати модуль автентифікації на основі розробленого протоколу, забезпечивши підвищену стійкість.

Аналіз протоколів автентифікації

Залежно від міри довірчих стосунків між сервером та клієнтом, структури автентифікація може бути односторонньою або взаємною. Також розрізняють однофакторну та строгу (двофакторну) автентифікації. В одно-факторних системах, найпоширенішими в цей час є парольні системи автентифікації. Серед сучасних протоколів автентифікації слід розглянути наступні: MQV, OpenID Connect, Kerberos, протокол Шнорра знанням [3-6].

Протокол MQV є протоколом розподілу ключів з аутентифікацією сторін побудований на основі протоколу Діффі-Геллмана, який використовується при автентифікації користувачів сучасними месенджерами [3].

OpenID Connect створений на основі OAuth 2.0, який можна використовувати для безпечної автентифікації користувача на веб-сервері. У OpenID Connect вводиться поняття маркера ідентифікації, який являє собою маркер безпеки, що дозволяє клієнту перевіряти особистість користувача. Маркер ідентифікації також дозволяє отримати базові відомості про профіль користувача. Процес автентифікації передбачає використання додаткового сервера [4].

Протокол Kerberos застосовується у клієнт-серверних сполученнях з великою кількістю користувачів. Kerberos пропонує алгоритм взаємної автентифікації користувачів перед початком встановлення з'єднання. Для роботи Kerberos необхідна довірена третя сторона. Протокол базується на симетричних криптографічних алгоритмах. В ролі довіреної третьої сторони виступають центр видачі квитків та додатковий сервер для автентифікації [5].

Протокол Шнорра застосовує доведення з нульовим знанням для автентифікації користувача. За протоколом Шнорра користувач, що проходить автентифікацію повинен довести стороні сервера, що він володіє секретною інформацією без розкриття секрету при цьому. Протокол Шнорра застосовує проблему дискретного логарифмування для процесу автентифікації [6].

Серед розглянутих протоколів найкращі результати у стійкості проявив протокол Шнорра, який виявився стійким до сучасних мережевих атак, тому його модифікацію взято за основу для модуля автентифікації користувачів.

Результати розробки

Модуль автентифікації користувачів складається з серверної та клієнтської частин. Серверна та клієнтська частини обмінюються інформацією при автентифікації за допомогою протоколу HTTPS.

Серверна частина модуля складається з чотирьох основних компонентів: блок криптографічних перетворень, блоку керування серверною частиною, блоку взаємодії з базою даних та блоку обміну даними. Блок криптографічних перетворень забезпечує реалізацію криптографічних примітивів протоколу автентифікації. Блок виконує відповіді криптографічні перетворення для кожного з кроків автентифікації відповідно до протоколу автентифікації. Перетворення здійснюється над даними, що отримуються з блока керування, після чого криптографічний блок повертає результат на блок керування. Блок керування відповідає за обробку даних, що передаються з блока обміну даними. Блок керування формує команди для інших блоків, залежно від отриманих даних. Блок обміну даними забезпечує передачу інформації між серверною та клієнтською частиною модуля. Блок взаємодії з базою даних забезпечує можливість зв'язку модуля автентифікації з базою даних, де збережені параметри, що використовуються при автентифікації користувачів. Структура модуля автентифікації зображена на рисунку 1 .

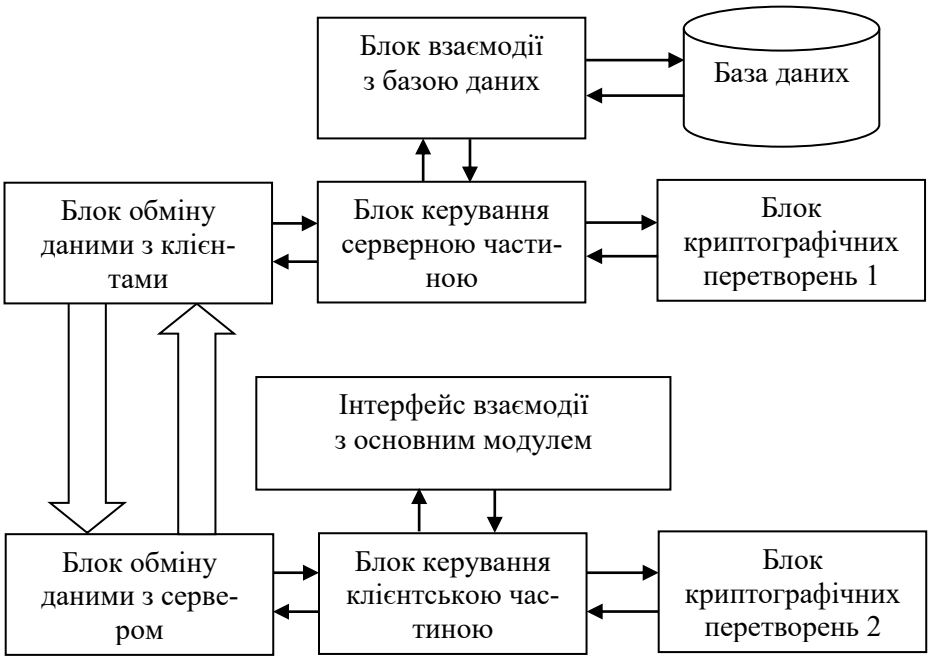

Рисунок 1 – Структура модуля автентифікації користувачів

Клієнтська частина модуля автентифікації складається з блоків обміну даними, керування та блоку криптографічних перетворень, що подібні до використаних на серверній частині, а також вістить інтерфейс для взаємодії з іншими модулями. Структура блоку криптографічних перетворень на клієнтській частині повністю збігається з його відповідною структурою на серверній частині. Блок обміну даними на клієнтській частині налаштований на зв'язок лише з серверною частиною, взаємодіє з

блоком керування, який формує відповідні команди для серверної частини, а також здійснює обробку отриманих від сервера відповідей. На основі цих відповідей та поточної команди блок керування надає команди для криптографічного блока у разі походження певного з кроків автентифікації. Інтерфейс для взаємодії з іншими модулями реалізує формування команд для блока керування, а також надають можливість відправлення блоком керування результатів автентифікації.

Модифікований протокол автентифікації з нульовим знанням передбачає використання операції множення, додавання, піднесення до степені за модулем та порівняння, які реалізовано у блоках криптографічних перетворень [7].

В якості протоколу автентифікації використано модифікований протокол з нульовим знанням, який застосовує поєднання двох математичних проблем: дискретне логарифмування та складність добування квадратного кореня за складеним модулем. Перед автентифікацією обирається модуль $n = pq$, що складається з двох великих простих множників, секретний ключ s, такий, що $1 \le s \le n-1$ та формуються два відкритих ключа за формулами $y_1 = \alpha^S \bmod n$ та $y_2 = s^2 \bmod n$, де α – випадкове число великого простого порядку $q < n$. Відкриті ключі $y1$ та $y2$ розподіляються між усіма учасниками протоколу. Виконання одного раунду автентифікації зображено на рисунку 2.

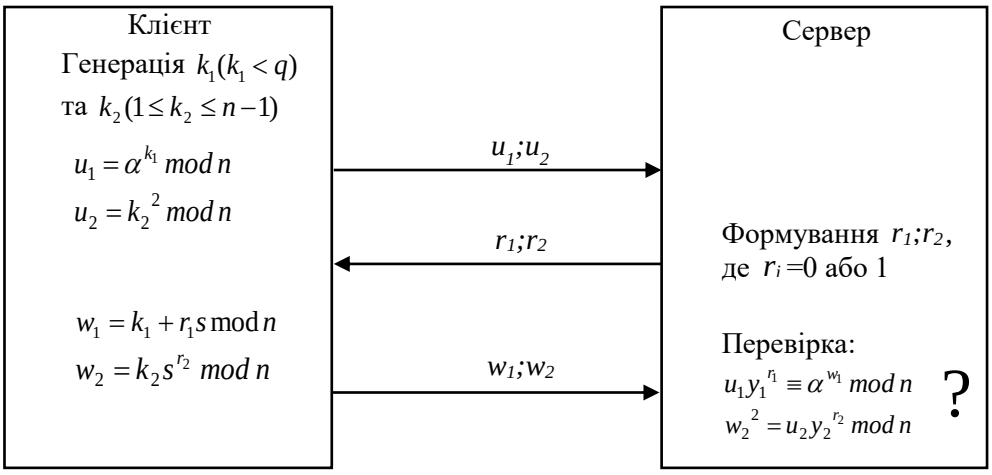

Рисунок 2 – Раунд протоколу автентифікації

Запропонований протокол автентифікації передбачає зменшення кількості раундів у порівнянні з оригінальними протоколами з нульовим знанням, а також у протоколі суттєво покращується стійкість при автентифікації.

Висновки

Розроблений модуль автентифікації дозволяє забезпечити підвищений захист користувачів на серверному застосунку. Модифікований протокол автентифікації з нульовим знанням дозволяє забезпечити більшу швидкодію при заданому рівні впевненості в автентичності іншої сторони в порівнянні з подібними протоколами, оскільки потребує менше раундів автентифікації. Використання модифікованого протоколу суттєво підвищує складність реалізації модуля, однак це не є суттєвим при програмній реалізації. Модуль автентифікації користувачів інтегровано до засобу захищеного обміну повідомленнями на основі псевдонедетермінованих криптографічних перетворень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баришев Ю. В. Метод автентифікації віддалених користувачів для мережевих сервісів / Ю. В. Баришев, В. А. Каплун. Інформаційні технології та комп'ютерна інженерія: наук.-техн. журнал. – 2014. – Том 30. – № 2. – с. 13-17.

2. Баришев, Ю. В. Кривешко К. І. Метод автентифікації користувачів комп`ютерної мережі з прив`язкою до параметрів робочої станції / Тези доповідей Третьої Міжнародної науково-практичної конференції «Інформаційні технології та коп‘ютерна інженерія», м. Вінниця, 29-31 травня 2012 р. – Вінниця : ВНТУ, 2012. – С. 187-188.

3. Грабінський Д. М. Вороніна А. В. Аналіз методів та протоколів розподілу криптографічних ключів / Вісник інженерної академії України № 3-4, 2013 – с. 50–56.

4. Платформа Microsoft Identity и протокол OpenID Connect: веб-сайт. URL: https://docs.microsoft.com/ru-ru/azure/active-directory/develop/v2-protocols-oidc#validate-the-id-token (дата звернення: 27.12.2020)

5. Б. Шнайер Глава 3. Основные протоколы. Протокол Kerberos / Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф, 2002. – 816 с.

6. И. Д. Сиганов. Доказательства с нулевым разглашением как метод аутентификации в веб-приложениях / Математические структуры и моделирование: науч.-техн. журнал. – 2016. – Том 40. – № 4. – с. 143–150.

7. Селезньов В. І. Баришев Ю. В. Протокол автентифікації з нульовим знанням / XLIX науково-технічної конференції підрозділів ВНТУ: Матеріали доповідей, Вінниця, 27-28 квітня 2020 р. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/view/9299 (дата звернення 28.12.2020).

Селезньов Віталій Ігорович — студент групи 1БС-20м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: seleznov.vitalii@kaskadb.com.ua

Науковий керівник – ***Баришев Юрій Володимирович*** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua

Seleznov Vitalii — Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : seleznov.vitalii@kaskadb.com.ua

Scientific supervisor – ***Baryshev Yurii*** — PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, yuriy.baryshev@vntu.edu.ua