УДК 004.056.52

В. І. Селезньов
Ю. В. Баришев

ПРОТОКОЛ АВТЕНТИФІКАЦІЇ З НУЛЬОВИМ ЗНАННЯМ

Вінницький національний технічний університет;

Анотація
Проаналізовано відомі протоколи автентифікації з нульовим знанням. Запропонований протокол автентифікації, що дозволяє підвищити стійкість односторонньої автентифікації.
Ключові слова: криптографічний протокол, автентифікація, доведення з нульовим знанням, нульовий розголос.

Abstract
The analysis of known zero-knowledge authentication protocols was performed. An authentication protocol was proposed to increase stability of one-sided authentication.
Keywords: cryptographic protocol, authentication, zero knowledge proof, zero publicity.

Вступ

Сучасні протоколи автентифікації побудовані на основі шифрів, геш-функцій або обчисленні певної складної математичної задачі. Вони не завжди дозволяють забезпечити достатній рівень стійкості при заданій швидкості. Окрім того, внутрішня структура цих протоколів відома, що дозволяє зловмиснику виконувати атаки на протокол за відомою структурою. Тому створення протоколу автентифікації з нульовим знанням з модифікованою структурою є актуальним питанням на сьогодні [1].

Метою дослідження є підвищення стійкості протоколу автентифікації з нульовим знанням.

Для досягнення мети необхідно:

- проаналізувати відомі протоколи автентифікації;
- обрати підхід до реалізації протоколу;
- реалізувати протокол, забезпечивши підвищену стійкість.

Аналіз протоколів автентифікації з нульовим знанням

У протоколах автентифікації з нульовим знанням користувач, що проходить автентифікацію (Аліса) повинен довести стороні сервера (Бобу), що він володіє секретною інформацією без розкриття секрету при цьому. Тобто при виконанні процесу автентифікації відбувається нульовий розголос секрету Аліси. На сьогодні найпопулярнішими протоколами автентифікації з нульовим знанням є протокол Шнорра та протокол Фіата-Шаміра з різними модифікаціями [2].

Протокол Шнорра застосовує проблему дискретного логарифмування для процесу автентифікації [2, 3]. Спочатку відкритий ключ Аліси обчислюється з секретного ключа x за формулою $y = \alpha^x \bmod p$, де p – достатньо велике випадкове число; α – випадкове число великого простого порядку $q < p$. Процес автентифікації складається з декількох раундів, які в свою чергу складаються з трьох основних кроків:

1. Аліса обирає випадкове число $k(k < q)$, обраховує значення $R = \alpha^k \bmod p$ та передає Бобу.
2. Боб формує випадковий біт r та передає Алісі.
3. Аліса обчислює $w = k + rx$ та відсилає Бобу. Боб виконує перевірку співвідношення:

$$Ry^r \equiv \alpha^w \bmod p \qquad (1)$$

У разі істини співвідношення 1 Аліса успішно проходить автентифікацію. При такій схемі існує два можливих варіанта дій порушника, при який ймовірність дати правильну відповідь складає 0.5. При виконанні декількох раундів протоколу ця ймовірність суттєво зменшується і обчислюється за формулою 2^{-Z}, де Z – кількість раундів.

Протокол Фіата-Шаміра заснований на складності добування квадратного кореня за складеним модулем, що включає не менше двох великих простих множників, при умові, що множники збережено в секреті [3, 4]. Перед процесом автентифікації обирається модуль $n = pq$, секретний ключ s, такий, що $1 \le s \le n-1$ та обчислюється відкритий ключ $y = s^2 \bmod n$, відомий для всіх учасників протоколу. Подібно до протоколу Шнорра процес автентифікації проходить у декілька раундів та складається з трьох основних кроків:

1. Аліса обирає випадкове число $k(1 \le k \le n-1)$, обраховує значення $u = k^2 \bmod n$ та передає Бобу.
2. Боб формує випадковий біт r та передає Алісі.
3. Аліса обчислює $w = ks^r \bmod n$ та відсилає Бобу. Боб виконує перевірку співвідношення:

$$w^2 = uy^r \bmod n \qquad (2)$$

У разі істини співвідношення 2 Аліса успішно проходить автентифікацію. Ймовірність порушника успішно пройти автентифікацію за протоколом Фіата-Шаміра, що виконується Z раундів дорівнює відповідній ймовірності протоколу Шнорра та обчислюється за формулою 2^{-Z}. Протокол Фіата-Шаміра забезпечує більшу швидкість виконання у порівнянні з протоколом Шнорра, що забезпечується меншим обсягом обчислень [5].

Результати розробки

Розглянуті протоколи автентифікації з нульовим знанням використовують операції множення, додавання, піднесення до степеня за модулем, що дозволяє виконати об'єднання двох підходів для створення стійкого протоколу автентифікації. Оскільки структура протоколів Фіата-Шаміра та Шнорра також подібна, то доцільно її зберегти з об'єднанням у протоколі двох відкритих ключів на основі єдиного закритого з використанням для них схем відповідних до оригінальних протоколів [6].

Перед процесом автентифікації 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. Розпочинається процес автентифікації, що описаний декількома раундами, які складаються з наступних кроків:

1. Аліса обирає два випадкових числа $k_1(k_1 < q)$ та $k_2(1 \le k_2 \le n-1)$, обчислює значення $u_1 = \alpha^{k_1} \bmod n$ та $u_2 = {k_2}^2 \bmod n$, які передає Бобу.
2. Боб формує два випадкових біта $r_1; r_2$ та передає Алісі.
3. Аліса обчислює $w_1 = k_1 + r_1 s$ та $w_2 = k_2 s^{r_2} \bmod n$, які відсилає Бобу.
4. Боб виконує перевірку співвідношень $u_1 y_1^{r_1} \equiv \alpha^{w_1} \bmod n$ та ${w_2}^2 = u_2 {y_2}^{r_2} \bmod n$. У разі істини кожного з них можна перейти до наступного раунду, якщо ж хоча б одне з співвідношень хибне, то користувач не знає секретний ключ s, а процес автентифікація завершується з невтішним результатом.

Запропонований протокол автентифікації передбачає зменшення кількості раундів у порівнянні з оригінальними протоколами, оскільки ймовірність для порушника дати правильну відповідь і успішно пройти автентифікацію складає 4^{-Z}, де Z – кількість раундів. Таким чином у протоколі суттєво покращується стійкість при автентифікації. Процес виконання автентифікації [7], побудований за описаним протоколом доцільно розпаралелити, що суттєво покращить швидкодію протоколу.

Висновки

Отже, протоколи автентифікації з нульовим знанням дозволяють встановити істинність твердження і при цьому не передавати будь-якої додаткової інформації про саме твердження. Розроблено протокол, що об’єднує два відомих протоколи Фіата-Шаміра та Шнорра, а також потребує меншої кількості кроків порівняно з аналогічними протоколами автентифікації з нульовим знанням, що дозволяє забезпечити більшу швидкодію при заданому рівні впевненості в автентичності іншої сторони. Однак такий підхід ускладнює реалізацію засобу, заснованого на даному протоколі, що не є суттєвим при програмній реалізації засобу.

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. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. - CRC Press, 1996. - 816 с.
3. Усовершенствование протокола нулевых знаний, основанного на дискретных логарифмах / И.В. Олешко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – с. 363–372.
4. Молдовян А.А., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета.– СПб: Университет ИТМО, 2016. – 55 с.
5. И. Д. Сиганов. Доказательства с нулевым разглашением как метод аутентификации в веб-приложениях / Сиганов И. Д. // Математические структуры и моделирование: науч.-техн. журнал. – 2016. – Том 40. – № 4. – с. 143–150.
6. Лужецький В. А. Основи інформаційної безпеки: навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця: ВНТУ, 2013. – 201 с.
7. Баришев Ю. В. Моделі псевдонедетермінованих криптографічних перетворень / Ю. В. Баришев // Матеріали статей П’ятої Міжнародної науково-практичної конференції" Інформаційні технології та комп’ютерна інженерія", м. Івано-Франківськ, 27-29 травня 2015 р.: 189-190.

Селезньов Віталій Ігорович — студент групи 1БС-16б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: seleznov.vitalii@kaskadb.com.ua

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

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