УДК 004.056

РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ ДЛЯ АНАЛІЗУ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

DEVELOPMENT AND RESEARCH OF A SYSTEM FOR THE ANALYSIS OF CRYPTOGRAPHIC PROTOCOLS

Оксана Жигаревич, Максим Охочий, Іванна Шукалович

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *In this work, a software tool for generating and analyzing cryptographic protocols has been developed.*

Безпека криптографічних протоколів оцінюється через їх здатність гарантувати конфіденційність, цілісність і автентичність даних у моделі загроз Долева-Яо, яка передбачає наявність зловмисника, здатного контролювати та змінювати передачу даних. Конфіденційність досягається за допомогою асиметричного та симетричного шифрування, цілісність забезпечується за допомогою використання кодів автентифікації та підпису повідомлень, а автентичність перевіряється за допомогою схеми запит-відповідь і захисту від атак повтору. При аналізі безпеки криптографічних протоколів передбачається використання моделі загроз Долева-Яо, яка передбачає наявність зловмисника, який може контролювати передачу даних між сторонами, блокувати її, перехоплювати та змінювати всі повідомлення. Протокол повинен бути стійким до цього типу зловмисників і гарантувати секретність, достовірність і цілісність даних. Метою конфіденційності переданих даних є те, що зловмисник не може знати зміст даних, що передаються між юридичними сторонами.

Обмін ключами Діффі-Хеллмана, розроблений Вітфілдом Діффі та Мартіном Хеллманом у 1976 році, є цифровим методом шифрування, який дозволяє безпечно обмінюватися криптографічними ключами через загальнодоступний канал без передачі самих ключів. Використовуючи симетричну криптографію, цей метод захищає обмін ключами від атак типу "людина посередині" та забезпечує безпечне шифрування повідомлень, що використовується в таких протоколах, як TLS, SSH і IPsec.Необхідно використовувати попередньо спільний секретний ключ шифрування або генерувати його за допомогою протоколів для створення загального ключа сеансу, наприклад Діффі-Хеллмана. Мета цілісності переданих даних полягає в тому, щоб зловмисник не міг змінити дані, що передаються між юридичними сторонами. Метод не передає інформацію під час обміну ключами. Обидві сторони не мають попередньої інформації одна про одну, але дві сторони створюють ключ разом. Метою обміну ключами Діффі-Хеллмана є безпечне встановлення каналу для генерації ключів і обміну для алгоритмів симетричного ключа.

Метою роботи є розробка програмного засобу для генерування та аналізу криптографічних протоколів. Встановлена мета обумовлює наступні завдання: − генерування криптографічних протоколів на основі вибраних налаштувань; − реалізації програмної системи оцінки криптографічних протоколів; − моделювання роботи генерованого криптографічного протоколу.

Бібліографія

1. Decision and Complexity of Dolev-Yao Hyperproperties (Technical Report). Accueil - Archive ouverte HAL. URL: https://hal.science/hal-04261390/
2. A High-level Overview of Modern Cryptography. Cyphertalk. URL: https://muens.io/modern-cryptography-overview