УДК 621.391.7

Н. Ю. Шпортюк

АНАЛІЗ ВРАЗЛИВОСТЕЙ КРИПТОГРАФІЧНОЇ СХЕМИ ЦИФРОВОГО ПІДПИСУВАННЯ ECDSA

Вінницький національний технічний університет

Анотація

В роботі розглянуто та детально проаналізовано вразливість криптографічної схеми цифрового підписування ECDSA – генерація двох однакових цифрових підписів при використанні однієї і тієї ж пари сеансового та приватного ключів..

Ключові слова: сеансовий ключ, цифрове підписування, криптографія, ECDSA.

Abstract

The paper examines and details the vulnerability of the ECDSA cryptographic digital signature scheme - the generation of two identical digital signatures using the same pair of session and private keys.

Keywords*:* session key, digital signing, cryptography, ECDSA.

Вступ

У сучасному світі криптографічні методи широко застосовуються в системах безпеки. При цьому забезпечення цілісності на сьогодні є не менш актуальною задачею, ніж забезпечення конфіденційності інформації. Якщо задача конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілісності інформації використовують криптографічні протоколи. Найбільш розповсюдженими є протоколи цифрового підписування.

Метою роботи є аналіз вразливостей криптографічної схеми цифрового підписування ECDSA.

Результати дослідження

ECDSA (Elliptic Curve Digital Signature Algorithm) - алгоритм з відкритим ключем для створення цифрового підпису, аналогічний за своєю будовою DSA, але побудований, на відміну від нього, не над колом цілих чисел, а в групі точок еліптичної кривої.

Стійкість алгоритму шифрування ґрунтується на проблемі дискретного логарифма в групі точок еліптичної кривої. На відміну від задачі простого дискретного логарифма і задачі факторизації цілого числа, не існує субекспоненціального алгоритму для задачі дискретного логарифма в групі точок еліптичної кривої. З цієї причини «стійкість на один біт ключа» істотно вище в алгоритмі, який використовує еліптичні криві.

Алгоритм ECDSA в 1999 р був прийнятий як стандарт ANSI, в 2000 р - як стандарт IEEE і NIST. Також в 1998 р алгоритм був прийнятий стандартом ISO. Незважаючи на те, що стандарти ЕЦП створені зовсім недавно і знаходяться на етапі вдосконалення, одним з найбільш перспективних з них на сьогоднішній день є ANSI X9.62 ECDSA від 1999 - DSA для еліптичних кривих.

ECDSA є дуже легким алгоритмом для реалізації ЕЦП. Найважливішою перевагою ECDSA є можливість його роботи на значно менших полях F_p. Як, загалом, з криптографією еліптичної кривої, передбачається, що бітовий розмір відкритого ключа, який буде необхідний для ECDSA, дорівнює подвійному розміру секретного ключа в бітах. Для порівняння, при рівні безпеки в 80 біт (тобто атакуючому необхідно приблизно 2^{80} версій підписів для знаходження секретного ключа), розмір відкритого ключа DSA дорівнює, принаймні, 1024 біт, тоді як відкритого ключа ECDSA - 160 біт. З іншого боку розмір підпису однаковий і для DSA, і для ECDSA: $4t$ біт, де t - рівень безпеки, який вимірюється в бітах, тобто - приблизно 320 біт для рівня безпеки в 80 біт.

Для підписування повідомлень необхідна пара ключів - відкритий і закритий. При цьому закритий ключ повинен бути відомий тільки тому, хто підписує повідомлення, а відкритий - будь-кому для перевірки справжності повідомлення. Також загальнодоступними є параметри самого алгоритму.

На сьогоднішній день не відомо практично реалізованих атак при правильному виборі параметрів, хоча існує проблема пов’язана з можливим створенням однакового цифрового підпису для

двох різних повідомлень при використанні одного і того ж сеансового та приватного ключа, тому актуальним залишається питання і підвищення стійкості цих методів цифрового підписування.

Висновки

У даній роботі було детально проаналізовано криптографічну схему цифрового підписування ECDSA, розглянуто та описано її головні переваги та недоліки, до яких відноситься ймовірність генерації однакового цифрового підпису для двох різних повідомлень. Даний випадок можливий лише при виборі неправильних параметрів або при використанні статичного сеансового ключа.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гулак Г. М. Основи криптографічного захисту інформації / Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук – Вінниця, 2011 – 199 с.
2. Азаров О. Д.. Комп'ютерна криптографія / Азаров О. Д., Хорошко В. О., Шєлєст М. Є., Мухачьов В. А., Яремчук Ю. Є. - НАУ, 2003 – 14 с.
3. Ю. Є. Яремчук. Сучасний захист інформації / Ю.Є. Яремчук, А. П. Бондарчук, С. Я. Довбня, Ю. І. Хлапонін – Вінниця, 2013.
4. Cryptography [Electronic Resource]. – Mode of access : URL : https://en.wikipedia.org/wiki/Cryptography - Назва з екрану.
5. Elliptic Curve Digital Signature Algorithm [Electronic Resource]. – Mode of access : URL : https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm - Назва з екрану.

Шпортюк Назар Юрійович — бакалавр, Вінницький національний технічний університет, Вінниця, e-mail: shportyuk.nazar@gmail.com.

Науковий керівник: ***Яремчук Юрій Євгенович*** — доктор технічних наук, професор, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.

Shportiuk Nazar Yuriyovych — bachelor degree, Vinnitsa National Technical University, Vinnitsa, e-mail: shportyuk.nazar@gmail.com.

Supervisor: ***Yaremchuk Yuriy E***. — Ph. D., professor, management and security of information Systems department; Vinnitsa.