УДК 004.056

Андрюшков А. К.
Кирилащук Т. Г.

НАБОРИ ШИФРІВ CHACHA20-POLY1305 ДЛЯ ПРОТОКОЛУ ЗАХИСТУ ТРАНСПОРТНОГО РІВНЯ

Вінницький національний технічний університет

Анотація

У даних тезах досліджуються особливості використання наборів шифрів ChaCha20-Poly1305 у протоколах захисту транспортного рівня TLS та DTLS. Розглянуто недоліки традиційних криптографічних алгоритмів RC4 та AES-CBC, а також переваги сучасного підходу автентифікованого шифрування AEAD. Проаналізовано принцип роботи потокового шифру ChaCha20 та автентифікатора Poly1305, їхню стійкість до атак по сторонніх каналах і ефективність на пристроях без апаратної підтримки AES. Особливу увагу приділено механізму формування nonce, забезпеченню цілісності та конфіденційності даних, а також використанню ECDHE для реалізації досконалої прямої секретності. Показано, що використання ChaCha20-Poly1305 забезпечує високий рівень криптографічного захисту, продуктивності та апаратної незалежності сучасних мережевих систем.

Ключові слова: криптографічні файлові системи, GPU, шифрування даних, режим CTR, спекулятивне шифрування, продуктивність системи.

Abstract

The theses consider the features of using ChaCha20-Poly1305 cipher suites in the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols. The shortcomings of traditional cryptographic algorithms such as RC4 and AES-CBC, as well as the advantages of the modern AEAD authenticated encryption approach, are considered. The operating principles of the ChaCha20 stream cipher and the Poly1305 authenticator, their resistance to side-channel attacks, and their efficiency on devices without AES hardware acceleration are analyzed. Particular attention is paid to the nonce generation mechanism, ensuring data integrity and confidentiality, and the use of ECDHE to achieve Perfect Forward Secrecy. It is shown that the use of ChaCha20-Poly1305 provides a high level of cryptographic security, performance, and hardware independence for modern network systems.

Keywords: cryptographic file systems, GPU, data encryption, CTR mode, speculative encryption, system performance.

Вступ

Стрімкий розвиток мережевих технологій та зростання обсягів конфіденційної інформації вимагають постійного вдосконалення криптографічних протоколів. Довгий час основними механізмами захисту в протоколах TLS та DTLS залишалися набори шифрів на базі потокового алгоритму RC4 та блочного шифрування у режимі зчеплення блоків (CBC). Проте нещодавні криптоаналітичні дослідження виявили їхню фундаментальну вразливість. Зокрема, атака типу Lucky Thirteen продемонструвала критичні недоліки використання режиму CBC , а ряд атак на RC4 довів можливість повного відновлення відкритого тексту за рахунок статистичних зміщень у ключовому потоці.

На зміну цим алгоритмам прийшли набори шифрів з автентифікованим шифруванням (AEAD) на основі алгоритму AES у режимі лічильника з автентифікацією Галуа (AES-GCM). Хоча вони надійно вирішують описані проблеми безпеки, AES-GCM має суттєвий недолік: його програмна реалізація вимагає інтенсивних обчислень.

На апаратних платформах без вбудованої підтримки криптографічних інструкцій (таких як AES-NI) швидкість шифрування значно падає, а програмна реалізація через таб-личні підстановки робить систему вразливою до атак по сторонніх каналах (cache-timing attacks). У зв'язку з цим виникла нагальна потреба в новому потоковому шифрі для TLS та DTLS, який би забез-печував високу швидкість обчислень на мобільних і вбудованих пристроях, маючи при цьому високу криптографічну стійкість та апаратну незалежність.

Результати дослідження

Оптимальним рішенням стало впровадження комбінації алгоритмів ChaCha20 та Poly1305. ChaCha – це потоковий шифр, розроблений Д. Дж. Бернштейном як логічне вдосконалення алгоритму Salsa20 [1]. У цій реалізації використовується його найбільш консервативна та захищена версія з 20 раундами перетворень, 96-бітним одноразовим номером (nonce) та 256-бітним ключем.

Структурно ChaCha20 належить до класу ARX-алгоритмів (Addition, Rotation, XOR), що використовують лише прості базові операції: модульне додавання, циклічний зсув та логічне виключне АБО [1]. Завдяки відсутності S-блоків (таблиць підстановок) алгоритм виконується за строго визначений час, що робить його стійким до атак по часу виконання (timing attacks).

Забезпечення цілісності та автентичності даних покладено на алгоритм Poly1305 – одноразовий автентифікатор типу Вегмана-Картера, який також був створений Д. Дж. Бернштейном [2]. Він обробляє повідомлення будь-якої довжини з використанням 256-бітного одноразового ключа та генерує унікальний 16-байтовий криптографічний тег.

В ході дослідження примітиви ChaCha20 та Poly1305 було інтегровано в єдиний комплексний алгоритм автентифікованого шифрування з приєднаними даними – AEAD_CHACHA20_POLY1305 [1, 2]. Однією з найважливіших архітектурних особливостей цієї реалізації є механізм формування 96-бітного одноразового номера (nonce). Замість генерування випадкових значень, які необхідно передавати по мережі, запропоновано детермінований підхід. Згідно з ним, 64-бітний порядковий номер запису TLS серіалізується у 8-байтове значення у форматі big-endian та доповнюється зліва чотирма нульовими байтами (0×00). Після цього отримане 12-байтове значення виконує операцію XOR із 12-байтовим вектором ініціалізації клієнта (client_write_IV) або сервера (server_write_IV). Для протоколу DTLS цей номер складається з 16-бітної епохи та 48-бітного порядкового номера [3].

Такий підхід має три критичні переваги. По-перше, nonce формується з порядкового номера і спільного секрету, які вже відомі і відправнику, і одержувачу. Це усуває потребу передавати явний вектор ініціалізації у кожному мережевому пакеті, економлячи пропускну здатність мережі. По-друге, детерміноване формування повністю виключає помилки розробників програмного забезпечення, які могли б випадково згенерувати однакові значення nonce, що в потокових шифрах призводить до компрометації ключа. По-третє, такий підхід відповідає сучасним вимогам стандартів TLS [3].

Для забезпечення досконалої прямої секретності (Perfect Forward Secrecy) нові набори шифрів, наприклад TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, використовують механізм обміну ключами на базі еліптичних кривих Діффі-Геллмана (ECDHE). Як псевдовипадкову функцію (PRF) для всіх наборів обрано стійку криптографічну хеш-функцію SHA-256.

Висновки

У роботі розглянуто особливості використання наборів шифрів ChaCha20-Poly1305 у протоколах TLS та DTLS. Проведений аналіз показав, що даний криптографічний комплекс є ефективною альтернативою застарілим алгоритмам RC4 та AES-CBC, які мають ряд виявлених вразливостей. Використання потокового шифру ChaCha20 забезпечує високу швидкість роботи навіть на пристроях без апаратної підтримки AES, а алгоритм Poly1305 гарантує цілісність та автентичність переданих даних.

Важливою перевагою даного підходу є використання детермінованого механізму формування nonce, що дозволяє уникнути повторного використання одноразових значень та підвищує загальний рівень безпеки системи. Крім того, застосування механізму ECDHE забезпечує досконалу пряму секретність з'єднання.

Отримані результати підтверджують, що використання ChaCha20-Poly1305 є сучасним, швидким та криптографічно стійким рішенням для захисту мережевого трафіку, особливо для мобільних, вбудованих та високонавантажених систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Bernstein D. ChaCha, a variant of Salsa20. 2008. URL: http://cr.yp.to/chacha/chacha-20080128.pdf.
2. Bernstein D. The Poly1305-AES message-authentication code. 2005. URL: http://cr.yp.to/mac/poly1305-20050329.pdf.
3. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2 : RFC 5246. August 2008.

Андрюшков Артур Костянтинович – студент групи 2БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: arturandriuskow@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

Andriushkow Artur – student of group 2BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: arturandriuskow@gmail.com

Scientific Supervisor: ***Kyrylashchuk Tatyana*** – assistant of the Information Security Department, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com