УДК 004.056.53

Д. А. Дорофєєва
А. А. Шиян

РЕАЛІЗАЦІЯ ЗАХИЩЕНОГО ПРОТОКОЛУ ПЕРЕДАЧІ ДАНИХ З ВИКОРИСТАННЯМ МУЛЬТИ-ПАКЕТНОЇ ВЕРИФІКАЦІЇ ДЛЯ ПРОТИДІЇ АТАКАМ ТИПУ MAN-ON-THE-SIDE

Вінницький національний технічний університет

Анотація

У роботі розглянуто підхід до підвищення захищеності мережевої взаємодії на ранньому етапі встановлення TCP-з'єднання. Досліджено загрозу атак типу Man-on-the-side, за яких зловмисник, перебуваючи у позаканальній позиції, спостерігає за трафіком і намагається ін'єктувати підроблену відповідь раніше за легітимний сервер. Запропоновано механізм мульти-пакетної верифікації, у якому автентифікаційний токен фрагментується, обфускується та приховано передається у службових полях серії TCP SYN-пакетів. Сервер приймає рішення про легітимність сесії лише після отримання повної послідовності фрагментів і перевірки HMAC, що зменшує ризик успішної позаканальної ін'єкції.

Ключові слова: Man-on-the-side, мульти-пакетна верифікація, TCP/IP, Initial Sequence Number, HMAC, XOR-обфускація, мережева стеганографія, Zero Trust, Scapy, кібербезпека.

Abstract

The paper considers an approach to increasing the security of network communication at the early stage of TCP connection establishment. The threat of Man-on-the-side attacks is investigated, where an adversary observes traffic from an out-of-band position and attempts to inject a forged response earlier than the legitimate server. A multi-packet verification mechanism is proposed, in which an authentication token is fragmented, obfuscated, and covertly transmitted in service fields of a series of TCP SYN packets. The server makes a decision on session legitimacy only after receiving the complete fragment sequence and verifying the HMAC value, which reduces the risk of successful out-of-band injection.

Keywords: Man-on-the-side, multi-packet verification, TCP/IP, Initial Sequence Number, HMAC, XOR obfuscation, network steganography, Zero Trust, Scapy, cybersecurity.

Вступ

Сучасна мережева інфраструктура є основою функціонування державних, корпоративних і приватних інформаційних систем. Водночас розвиток глобальних систем моніторингу трафіку та поява атак класу Quantum Injection показали, що загрозу може становити не лише повне перехоплення каналу, а й позаканальне втручання у процес обміну пакетами [1, 2].

На відміну від атак типу Man-in-the-Middle, у моделі Man-on-the-side зловмисник не блокує легітимний трафік, а лише додає до потоку підроблений пакет. Успіх атаки визначається станом гонитви: якщо ін'єктована відповідь надходить до клієнта раніше за справжню відповідь сервера і має коректні службові параметри TCP-сесії, вона може бути прийнята як легітимна [1].

Традиційні засоби захисту не завжди усувають ризик на етапі ініціалізації сесії, оскільки частина службових метаданих може залишатися доступною для аналізу або використовуватися до завершення повної криптографічної перевірки. Тому актуальним є застосування принципів Zero Trust, за яких жоден окремий пакет не вважається достатньою підставою для довіри [3].

Метою роботи є розроблення підходу до захищеного встановлення мережевої сесії шляхом використання мульти-пакетної верифікації, фрагментації автентифікаційного токена та його прихованого передавання у службових полях TCP-заголовка.

Результати дослідження

Запропонований підхід ґрунтується на перенесенні автентифікаційної перевірки на початковий етап встановлення з'єднання. На відміну від стандартної логіки, за якої сервер реагує на перший SYN-пакет, у запропонованій моделі сервер очікує надходження серії TCP SYN-пакетів, що містять фрагменти автентифікаційного токена. Така схема зменшує залежність безпеки сесії від принципу "довіри до першої відповіді".

Автентифікаційний токен формується з урахуванням секретного ключа, часової мітки та випадкового значення nonce. Для підтвердження цілісності й автентичності використовується код автентифікації повідомлення HMAC, який дає змогу виявляти зміну фрагментів або спробу формування підробленої послідовності без знання спільного секрету [5].

Після формування токен розбивається на окремі фрагменти, кожен з яких додатково обфускується за допомогою XOR-операції. Обфусковані фрагменти розміщуються у полі Initial Sequence Number TCP-заголовка. Оскільки це поле є штатною частиною процесу встановлення TCP-з'єднання, такий спосіб дозволяє реалізувати елемент мережевої стеганографії без введення додаткового прикладного протоколу [4].

На стороні сервера реалізується буферизація прийнятих фрагментів. Позитивна відповідь не формується доти, доки не буде отримано повну серію пакетів, відновлено токен і виконано перевірку HMAC. Якщо хоча б один фрагмент відсутній, має неправильний порядок, надходить поза допустимим часовим вікном або не проходить перевірку цілісності, з'єднання відхиляється.

Ключовою перевагою моделі є ускладнення стану гонитви для атакуючого. Для успішної ін'єкції вже недостатньо перехопити один пакет і швидко сформувати підроблену відповідь. Зловмисник повинен коректно відтворити повну послідовність фрагментів токена, їх порядок, часові параметри та значення HMAC, що істотно підвищує складність атаки.

Для практичної перевірки підходу було розроблено програмний прототип засобами Python із використанням бібліотеки Scapy, яка дає змогу формувати, модифікувати та аналізувати мережеві пакети на рівні TCP/IP [6]. Тестування виконувалося у контейнеризованому середовищі з моделюванням взаємодії клієнта, сервера та позаканального атакуючого вузла.

Таблиця 1 - Узагальнення алгоритмічного забезпечення мульти-пакетної верифікації

Компонент або підхід	**Основне призначення**	**Очікуваний результат**
Фрагментація токена	Поділ автентифікаційних даних між кількома пакетами	Відсутність довіри до одного пакета
XOR-обфускація	Маскування фрагментів у службовому полі TCP	Зменшення очевидності службових даних
HMAC-перевірка	Контроль цілісності та автентичності токена	Відхилення підроблених послідовностей
Буферизація фрагментів	Очікування повної серії SYN-пакетів	Перехід до довіреного стану лише після перевірки
Fail-Safe логіка	Відхилення неповних або передчасних відповідей	Зниження ризику позаканальної ін'єкції

Висновки

У результаті дослідження обґрунтовано доцільність використання мульти-пакетної верифікації для протидії атакам типу Man-on-the-side. Запропонована модель змінює логіку встановлення довіри між клієнтом і сервером: рішення про легітимність сесії приймається не після першого пакета, а після перевірки повної послідовності автентифікаційних фрагментів.

Розроблений підхід поєднує фрагментацію токена, XOR-обфускацію, HMAC-перевірку та приховане передавання службової інформації через поле Initial Sequence Number. Це ускладнює реалізацію позаканальної ін'єкції, оскільки атакуючий повинен мати не лише часову перевагу, а й можливість коректно відтворити всю структуру автентифікаційної послідовності.

Практична реалізація прототипу на Python і Scapy підтвердила можливість використання запропонованого підходу в тестовому середовищі. Подальші дослідження доцільно спрямувати на

оцінювання стійкості методу в реальних мережевих умовах, оптимізацію кількості фрагментів токена та інтеграцію механізму з сучасними протоколами захищеної передачі даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Brooker M. Quantum Insert Analysis [Електронний ресурс] / M. Brooker // Fox-IT. - 2015. - Режим доступу: https://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/
2. Deep Dive into NSA's Turmoil and Turbine Surveillance Architecture [Електронний ресурс] // CTF-IoT Information Security. - 2023. - Режим доступу: https://www.ctfiot.com/171980.html
3. Rose S. Zero Trust Architecture [Електронний ресурс] / S. Rose, O. Borchert, S. Mitchell, S. Connelly // NIST Special Publication 800-207. - 2020. - Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
4. Eddy W. Transmission Control Protocol (TCP) [Електронний ресурс] / W. Eddy // IETF. - 2022. - RFC 9293. - Режим доступу: https://datatracker.ietf.org/doc/html/rfc9293
5. Krawczyk H. HMAC: Keyed-Hashing for Message Authentication [Електронний ресурс] / H. Krawczyk, M. Bellare, R. Canetti // IETF. - 1997. - RFC 2104. - Режим доступу: https://datatracker.ietf.org/doc/html/rfc2104
6. Scapy documentation [Електронний ресурс]. - Режим доступу: https://scapy.readthedocs.io/

Дорофєєва Діана Аркадіївна - студентка групи 2КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: doroofaa@gmail.com

Шиян Анатолій Антонович - к.ф.-м.н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: shyian@vntu.edu.ua

Dorofieieva Diana A. - student of group 2KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: doroofaa@gmail.com

Shyian Anatolii A. - PhD, Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: shyian@vntu.edu.ua