УДК 004.056.55

МОДИФІКАЦІЯ МЕТОДУ АУТЕНТИФІКАЦІЇ ДЛЯ СТВОРЕННЯ ПРИХОВАНОГО КАНАЛУ В SDN

Фокін Д.Г.
e-mail: denys.fokin@nure.ua
Науковий керівник – д.т.н., проф. Євдокименко М.О.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна

This paper describes the modification of an information hiding-based authentication mechanism in Software-Defined Networks (SDN) to establish a covert communication channel. The original method utilizes the IPID field of the IPv4 header to hide network devices' unique identifiers. This mechanism was modified by introducing a two-ID approach, where two distinct IDs represent binary '1' and '0', enabling the bit-by-bit transmission of arbitrary text messages instead of an authentication check. The modified covert channel was evaluated on a Mininet virtual testbed with a Ryu controller. A 512-byte covert message was successfully transmitted at a speed of 12.56 bps with a 0% error rate.

Програмно-конфігуровані мережі (Software-Defined Networks, SDN) відокремлюють логіку управління від пристроїв передачі даних, що забезпечує гнучкість, але створює потенційні загрози безпеці, такі як атаки типу "відмова в обслуговуванні" (DoS).

Для захисту каналу управління в роботі [1] було запропоновано легкий механізм аутентифікації на основі приховування інформації. Оригінальний метод використовує поле ідентифікації IP (IPID) протоколу IPv4 для приховування унікальних ідентифікаторів (UID) мережних пристроїв. Механізм аутентифікації виглядає наступним чином:

1. Мережному пристрою, наприклад, комутатору, призначається 16-бітний UID.
2. Обирається 16-бітна випадкова послідовність, наприклад, 2 байти з ідентифікатора транзакції OpenFlow (xid).
3. Виконується XOR між UID та xid.
4. Отриманий 16-бітний результат використовується як індекс у попередньо згенерованій та розділеній між пристроями таблиці підстановки. Значення з таблиці визначає кінцевий IPID, який записується у заголовок пакета. На стороні приймача, наприклад, контролера, цей процес виконується у зворотному порядку для вилучення та перевірки UID.

Однак цей підхід розрахований лише на успішну або неуспішну аутентифікацію. Для того, щоб використовувати цей алгоритм як прихований канал передачі повідомлень, виникла потреба у його модифікації, оскільки оригінальний механізм не передбачав можливості передачі довільних даних.

Було модифіковано цей метод, впровадивши підхід двох ідентифікаторів. Замість одного UID було використано два: перший представляв біт '1', а другий – біт '0'.

1. Для кожного біта повідомлення обирається відповідний UID.

2. Обраний UID проходить через оригінальний алгоритм (XOR із xid пакета та пошук у таблиці підстановки) і формує значення поля IPID для одного вихідного OpenFlow-пакета. Таким чином, кожен пакет переносить рівно 1 біт корисної інформації.

3. Отримувач перехоплює пакети, за допомогою зворотної таблиці та операції XOR відновлює UID, визначає значення поточного біта і накопичує їх.

Метод було протестовано на віртуальному стенді за допомогою емулятора Mininet з контролером Ryu. Один с хостів в мережі генерував фоновий трафік за допомогою утиліти tcpreplay з набору даних InSDN [2]. На стороні відправника міжпакетна затримка 10 мс для запобігання доставці поза порядком. Як результат, повідомлення розміром 512 байт було передано зі швидкістю 12.56 біт/с з рівнем помилок 0%.

Переваги методу:

- висока прихованість: оскільки генерація IPID не має жорстких вимог у специфікації RFC, пакети виглядають як звичайний мережний трафік.

- стійкість до шуму: є можливість реалізувати BPF-фільтр для стабільної роботи під час великого навантаження, наприклад, DoS-атак.

Недоліки методу:

- низька пропускна здатність: кожен пакет може передати лише 1 біт корисної інформації;

- вразливість до втрати пакетів: якщо один стеганографічний пакет буде втрачено, весь наступний текст буде розшифровано некоректно через зсув бітів.

Подальше вдосконалення методу може включати впровадження маркерів синхронізації або використання кодів корекції помилок для запобігання пошкодження повідомлення через втрату пакеті, а також, динамічну зміну таблиць підстановки для ускладнення виявлення стеганографії.

Список використаних джерел:

1. Abdullaziz O. I., Chen Y.-J., Wang L.-C. Lightweight Authentication Mechanism for Software Defined Network using Information Hiding. *2016 IEEE Global Communications Conference (GLOBECOM)*. Washington, DC, 2016. P. 1–6.

2. Elsayed M. S., Le-Khac N.-A., Jurcut A. D. InSDN: A Novel SDN Intrusion Dataset. *IEEE Access*. 2020. Vol. 8. P. 165263–165284. DOI: 10.1109/ACCESS.2020.3022633.