УДК 004.056

КЛАСИФІКАЦІЯ І МЕТОДИ ПРОТИДІЇ ЗАГРОЗ, НАЦІЛЕНИХ НА DATA PLANE І CONTROL PLANE

А. О. Дорош[1], В. В. Демчинський[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У роботі проведено аналіз векторів атак на SDN мережі, що були категоризовані за допомогою методики STRIDE, а також вказано відповідні методи протидії. На основі імплементації такої мережі були розроблені практичні поради щодо її ефективного впровадження та захисту.

Ключові слова: Software-defined network, STRIDE, моделювання загроз, SDN hardening

Вступ

Людство пройшло довгий шлях у побудові зручних і надійних методів комунікації. Хоча так звані «класичні» мережі вже стали стандартом, на заміну їм поступово приходять програмно-визначені мережі, що більш відомі під абревіатурою SDN (Software Defined Networking). До компаній-гігантів, що вже опанували і використовують цю технологію на повну можна віднести Amazon [1] і Google [2].

Основною особливістю SDN є розмежування обов'язків щодо керування мережею на три рівні: Data Plane, Control Plane і Application Plane [3]. Перший (Data Plane) складається з фізичних комутаторів у мережі. Ці комутатори пересилають мережеві дані до своїх цілей. Другий (Control Plane) діє як основний центр керування. Останній (Application Plane) складається із додаткових допоміжних сервісів. Сюди входять системи виявлення вторгнень, балансування навантаження, брандмауери, тощо.

Комунікація між цими рівнями забезпечується через Southbound і Northbound відповідно (рис.1).

Проте вирішуючи одні проблеми, сучасні мережеві інженери і інженери із інформаційної безпеки стикаються з новими викликами і новими векторами атак.

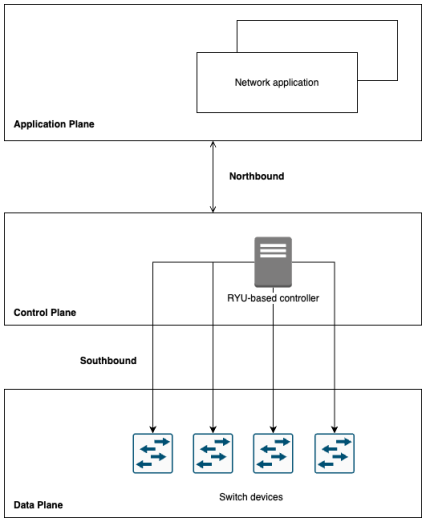

Рис. 1. Розподіл мережі на рівні у SDN

1. Опис тестової моделі та використаних інструментів

Для проведення експерименту були використані наступні інструменти:

- Ryu у якості фреймворку для написання контролеру;
- Mininet для емуляції пристроїв у Data Plane;
- DELTA – допоміжний фрейморк для поведення тестів на проникнення;

Топологія мережі є дуже спрощеною і складається із одного контролера і 4 SDN комутаторів (рис.1).

Для класифікації розглянутих загроз була використана модель STRIDE. Такий розподіл на 6 категорій дозволить якісніше і точніше охарактеризувати ландшафт потенційних загроз.

Важливо зауважити, що у роботі були розглянуті загальні атаки, що притаманні не конкретним вендорам або інструментам, а радше SDN як концепції.

2. Spoofing

У контексті STRIDE, Spoofing означає підроблення автентифікаційних даних користувача, щоб здійснити несанкціонований доступ до системи.

Sybil attack

Sybil attack – це тип атаки, в якій зловмисник створює кілька фальшивих ідентифікаторів або вузлів у мережі, щоб отримати контроль над нею.

У SDN вона зазвичай означає підробку одного або декількох пристроїв у Data plane. Ці фейкові вузли можуть надсилати шкідливий трафік або інструкції

легітимним вузлам мережі, змушуючи їх виконувати дії, які вигідні зловмиснику.

Методи протидії: впровадження надійних механізмів автентифікації і використання "reputation-based" систем.

Controller Spoofing

Атака, що є схожою на попередню, проте націлена на Control Plane, тобто на підміну SDN контролерів. Видаючи себе за легітимний контролер, зловмисник може отримати контроль над мережею та маніпулювати її поведінкою.

Методи протидії: впровадження надійних механізмів автентифікації та використання криптографічних протоколів для захисту зв'язку між контролерами та комутаторами. Крім того, рекомендується розгорнути IDS/IPS для виявлення і запобігання будь-якого несанкціонованого доступу до мережі.

Switch Identification Spoofing

Дана атака полягає в тому, що зловмисник намагається ввести контролер в оману, видаючи себе за інший комутатор або пристрій в мережі, і націлена на Data Plane.

Хоча з першого погляду Sybil Attack і Switch Identification Spoofing мають схожий принцип роботи, їх різниця полягає у підході до виконання: перша передбачає створення декількох фальшивих ідентифікаційних даних для отримання впливу в мережі, тоді як друга полягає в тому, що зловмисник видає себе за інший, вже існуючий пристрій в мережі.

Методи протидії: зважаючи на особливості атаки, доречним буде впровадження механізмів автентифікації комутаторів. Додаткові рекомендації включаються в себе шифрування зв'язку між контролерами та комутаторами і розгортання IPS/IDS систем.

MiTM

Атака Man-in-the-Middle є загрозою як для класичних мереж, так і для SDN. Вона полягає у розміщенні зловмисника між легітимними відправником і отримувачем. Таким чином, він отримує змогу переглядати, змінювати та перенаправляти трафік у мережі, або навіть викликати перенавантаження, а отже і відмову у обслуговуванні.

Методи протидії: насамперед це шифрування каналів зв'язку між вузлами мережі, а також методів автентифікації. Також можливо запровадити власні програмно-прописані алгоритми захисту напряму у контролері [4].

3. Tampering

Несанкціоноване втручання (tampering) – це тип атак, що в контексті SDN передбачає несанкціоновану зміну або модифікацію даних, налаштувань або інших ресурсів на будь-якому із трьох рівнів мережі.

Link Fabrication

Однією зі складових ефективного керування як мережею, так і її безпекою є видимість хостів та зв'язків між ними. Дана атака націлена на спотворення топології мережі і підробку зв'язків між пристроями, що може призвести до перенаправлення трафіку на зловмисний хост, який виступає у ролі віртуальної ланки між двома вузлами.

Методи протидії: використання HMAC [5] – hash-based message authentication code - для збереження цілісності повідомлень, а також перевірка станів портів, що виявляє розбіжності між заявленими властивостями портів та реальними можливостями мережевих пристроїв.

Host Location Hjacking

Розповсюдженою практикою серед проектування SDN контроллерів є використання Host Tracking Services, що дозволяє контролеру відстежувати місцезнаходження хостів у мережі.

Працює він наступним чином: коли до мережі приєднується новий хост або існуючий хост змінює місцеположення, служба відстеження хостів відповідно оновлює топологію мережі, і контролер може переконфігурувати мережеві шляхи, щоб забезпечити доставку пакетів за призначенням [6].

Атака полягає у перереєстрації місцеположення хоста у мережі, що призводить до перенаправлення трафіку до зловмисника.

Методи протидії: можна віднести сегментацію мережі для зменшення поверхні атаки, регулярний аудит і моніторинг, а також відстеження та верифікацію хостів. Рекомендується також використання спеціалізованого ПЗ, а саме TopoGuard [5] і SPHINX [7].

Port Amnesia

Вона використовує повідомлення OpenFlow для скидання поведінкового профілювання [6]. Таким чином, зловмисник може скинути дані про певний порт за допомогою виклику Port-Down повідомлення. Загалом, до такого типу атак вразливі всі методи захисту, що використовують профілі портів і очищають їх на основі повідомлень OpenFlow.

Методи протидії: основна стратегія – це фільтрація пакетів для відсіювання зловмисного трафіку до того, як він потрапить на комутатор.

Flow Table Manipulation

У програмно-визначених мережах (SDN) таблиця потоків (Flow table) – це структура даних, за допомогою якої комутатори зберігають правила передачі мережевої інформації.

Записи у такій таблиці (Flow entry) вказують, як обробляти різні типи мережевих даних. Кожен елемент потоку має набір полів відповідності та дій, які з ними пов'язані. Поля відповідності містять інформацію про пакети, які надходять, в той час як дії вказують комутатору, що робити з пакетами. За керування і внесення записів у таблицю потоків відповідає контролер.

Загалом можна винести два основі підтипи даної атаки [8]: модифікація даних у таблиц і видалення даних із таблиці.

Методи протидії: налаштування списків контролю доступу (ACL), а також імплементація системи виявлення мережевих вторгнень (NIDS) і системи для аналізу мережевої поведінки поведінки (NBA).

Malformed Message

Робота OpenFlow підтримується завдяки використанням повідомлень [9]. Їх стандартна структура відкриває два шляхи для атаки: модифікація заголовку (тобто полів version, type, message length, transaction ID) або ж модифікація тіла (payload).

Також такі атаки можна класифікувати за підходом:

1. Зміна певного параметру для впливу на вже існуючу конфігурацію;
2. Введення некоректних даних, наприклад, у поле довжини повідомлення, що може призвести до припинення роботи вузла у мережі.

Методи протидії: оскільки маніпуляції над повідомленнями можуть бути складовою також раніше згаданої MiTM атаки, методи захисту теж перетинаються. Додатково необхідно прописування чітких політик керування винятками (exceptions) для уникнення непередбачуваних реакцій на інциденти.

4. Repudiation

У STRIDE дана категорія означає можливість суб'єкта заперечувати виконання певної дії. Це може бути проблемою, коли йдеться про забезпечення цілісності та аудиту системи.

За відсутності налаштувань моніторингу та логування системи для атакуючого відкривається можливість непомітно виконувати дії у системі. Для різних вендорів і загалом типів контролерів притаманні свої особливості, що і впливають на вибір оптимального рішення.

5. Information disclosure

Розголошення інформації (information disclosure) є потенційною загрозою, яка може виникнути, коли конфіденційна інформація, стає доступною неавторизованим особам.

Eavesdrop

Як було згадано раніше, крім самих вузлів мережі, слабкими місцями можуть бути і канали комунікації. Eavesdrop є підвидом MiTM атаки і зосереджена на перехопленні та моніторингу мережевого трафіку з метою збору інформації, тобто без маніпуляцій над змістом. Найчастіше у зоні ризику прапляється насамперед Data Plane, а також Southbound in Northbound інтерфейси, тобто канали комунікації між рівнями.

Методи протидії: шифрування каналів зв'язку та політики контролю доступу.

6. DoS

Атаки цієї категорії – відмови у обслуговуванні (Denial-of-Service) - напряму впливають на одну зі складових CIA-тріади, а саме доступність.

Flow table flooding

Атака націлена на Data Plane, а саме на переповнення пам'яті для зберігання правил потоку (Flow rules). Таким чином збільшується навантаження на мережу, а отже і до перевантаження і до припинення роботи сегменту мережі.

Приклад атаки виглядає наступним чином: скомпроментований хост надсилає безперервні table-miss запити, таким чином змушуючи комутатор надіслати Packet-In повідомлення до контролеру. У відповідь контролер генерує Flow-Mod повідомлення, що містять у собі правила (Flow entry), що власне і переповнюють таблицю (Flow Table).

Методи протидії: основою таких проблем зазвичай є проблеми ще на етапі проєктування мережі. Тому надійними методами є впровадження алгоритмів для керування записами [10].

7. Elevation of privilege

Підвищення привілеїв (Elevation of Privilege, EoP) відбувається, коли користувач або зловмисник отримує більше доступу або дозволів, ніж йому дозволено.

Controller hijacking

Даний тип атаки передбачає нелегітимне отримання доступу до SDN-контролеру, а також, відповідно, контроль над мережею. Вдала атака може слугувати стартовою точкою для подальших неправомірних дій, крадіжки даних, а також стати причиною значних збитків і навіть припинення роботи мережі в цілому.

Методи протидії: розгортання надійних механізмів автентифікації та контролю доступу до SDN контролера, часті оновлення ПЗ для усунення виявлених вразливостей та використання методів шифрування для захисту мережевого трафіку. Крім того, адміністраторам необхідно проводити ретельний моніторинг мережі для виявлення будь-якої аномальної діяльності або сумнівної поведінки.

8. Практичні рекомендації до захисту SDN мережі

На основі аналізу атак на технології SDN, відповідних методів протидії та експериментального впровадження було сформульовано рекомендації та практичні поради щодо розгортання та захисту такого типу мереж.

Архітектурні рішення

Запровадження механізмів захисту починається не із запуску системи, а ще на початку її проєктування. Оскільки SDN дозволяє самостійно проєктувати контролери, це дозволяє підлашувати рішенння під конкретні цілі. Наприклад, аби імплементувати алгоритми керування записами [10] у Flow Table для попередження DoS атак.

Захист каналів зв'язку між вузлами мережі

Один із варіантів для класичних мереж – TLS, однак цей метод може негативно впливати на продуктивність мережі [11]. Одна із альтернатив – еліптична криптографія (ECC). Проте дослідження все ще тривають і вибір методу шифрування залежить від наявного плану і кількості пристроїв.

Автентифікація

Автентифікація пристроїв гарантує, що тільки легітимні комутатори та контролери можуть брати участь в мережевому спілкуванні. Рекомендується використовувати цифрові сертифікати або ж, наприклад, PKI перед тим, як дозволити пристроям приєднатися до мережі SDN.

Моніторинг

Перший етап у якісному реагуванні на інциденти - отримання оперативної інформації про стан системи. Тому якісний моніторинг є його основою. Сюди можна віднести системи різних класів, а саме: SIEM + SOAR для збору та аналізу логів; (N)IDS/IPS для детектування і попередженя вторгнень; NBA для аналізу аномалій трафіку; deception системи для збільшення поверхні атаки тощо.

Використання спеціалізованого ПЗ

Окрім засобів, використання яких вже стало стандартом для класичних мереж, також є набір вузьконаправлених механізмів саме для SDN. Наприклад, раніше згадані TopoGuard [5] і SPHINX [7]. Перше рішення виявляє фальшиві мережеві з'єднання і підроблені кінцеві хости за допомогою поведінкового профілювання і інваріантного тестування, в той час як друге покладається на розбіжності у стані мережі на різних, заздалегідь розташованих, датчиках для визначення аномалій.

Висновки

В роботі розглянуто загальні вектори атак на технології SDN мереж, проведено їх аналіз та класифікацію на основі STRIDE, що дало можливість деталізувати аспекти застосування відповідних механізмів захисту. В результаті побудови типової SDN мережі надано рекомендації для більш ефективного її налаштування та практичні поради щодо впровадження механізмів захисту.

Перелік використаних джерел

1. *Shackleford D.* Adopting a softwaredefined network fabric in AWS. — 05.2020.
2. *Google.* Inter-Datacenter WAN with centralized TE using SDN and OpenFlow. — 07.2012.
3. *ONF.* SDN Architecture 1.0 Overview. — 12.2016.
4. Detection and Mitigation of MITM Attack in Software Defined Networks / A. KV [та ін.]. — 2021.
5. Poisoning network visibility in software-defined networks: New attacks and countermeasures. / S. Hong, L. Xu, H. Wang, G. Gu // Ndss. T. 15. — 2015. — С. 8—11.
6. Effective topology tampering attacks and defenses in software-defined networks / R. Skowyra, L. Xu, G. Gu, V. Dedhia, T. Hobson, H. Okhravi, J. Landry // 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). — IEEE. 2018. — С. 374—385.
7. Sphinx: detecting security attacks in software-defined networks. / M. Dhawan, R. Poddar, K. Mahajan, V. Mann // Ndss. T. 15. — 2015. — С. 8—11.
8. Flow wars: Systemizing the attack surface and defenses in software-defined networks / C. Yoon, S. Lee, H. Kang, T. Park, S. Shin, V. Yegneswaran, P. Porras, G. Gu // IEEE/ACM Transactions on Networking. — 2017. — Т. 25, № 6. — С. 3514—3530.
9. *ONF.* OpenFlow Switch Specification. — 04.2013.
10. *Duy P. T., An L. D., Pham V.-H.* Mitigating flow table overloading attack with controller-based flow filtering strategy in SDN // Proceedings of the 2019 the 9th International Conference on Communication and Network Security. — 2019. — С. 154—158.
11. *Durner R., Kellerer W.* The cost of security in the SDN control plane // ACM CoNEXT 2015-Student Workshop. — 2015.