УДК 621.391

ЗАГРОЗИ БЕЗПЕЦІ У SDN СЕРЕДОВИЩАХ

Роговий В.П.
Інститут телекомунікаційних систему КПІ ім. І. Сікорського, Україна
E-mail: vitalii.rohovyi@gmail.com

Security threats in SDN environments

Networks based on the Software-Defined Networking (SDN) technology has the same security problems as traditional analogues. The description of main network attacks typical to SDN networks is presented in this paper.

Мережі, що працюють на базі технології програмно-визначених мереж (SDN) все ще мають такі ж вимоги до безпеки, що й традиційні мережеві інфраструктури, так як вони переносять таку ж приватну та конфіденційну інформацію. SDN повністю змінює архітектуру та міжкомунікаційні особливості компонентів в мережі - з цього виникає зовсім новий «стартовий майданчик» для зловмисників, які бажають атакувати SDN-мережі. Це призводить до необхідності підтримання аналогічного рівня безпеки як при використанні традиційних мереж, але потрібно ще зважати на небезпеки програмної природи. Далі у статті будуть приведені деякі загрози, що становлять небезпеку й в SDN мережах.

A. DDoS / DoS атаки.

1) DDoS (Distributed Denial-of-Service): численні типи звичайних атак DDoS можуть виконуватися і в SDN середовищі, але це вже буде варіація атаки з використанням підроблених записів потоку, яка може бути націлена супротивником на контролер, а саме на компрометування його доступності. Флудінг контролеру запитами щодо рішення вибору потоку призводить до того, що обчислювальні ресурси контролеру можуть перевантажитись, і контролер не зможе відповідати на коректні запити. Якщо атакованою буде централізована точка керування мережею, а саме таким пристроєм є SDN-контролер, то частина мережі, що підпорядкована цьому контролеру буде доступною тільки деякий малий період часу, поки мережеві пристрої (МП) по тайм-ауту не опитають контролер щодо нових правил у мережі. Після того, як МП не отримали відповідь контролеру під атакою, вони чи обнуляють свої таблиці комутації/маршрутизації, чи використовують попередні версії цих таблиць. Це призводить до «падіння» мережі.

2) DoS (Denial-of-Service): на рівні площини даних інші МП можуть бути підвержені флудінгу помилково створеними записами потоків, котрі займають все вільне місце в таблиці потоків. Це призведе до того, що маршрутизуючі МП не зможуть додати будь-які коректні записи потоків в свої таблиці і частина мережі стане розрізненою. Одна з основних проблем з пристроями на рівні площини даних в мережах SDN полягає в неможливості комутаторів розрізняти коректні запити щодо потоків від скомпрометованих.

B. Викрадений / підроблений контролер. Контролер можна розглядати як централізований "мозок" мережі SDN. Він контролює всю мережу з однієї точки, що робить це найважливішою особливістю SDN архітектури. Зловмисник, якому вдається скомпрометувати контролер по суті контролює всю мережу. Можливість контролювати дії контролера дозволить зловмиснику маніпулювати даними потоків будь-яким способом, який він обере, наприклад, може припини передачу певних типів даних на деякі кінцеві вузли та перенаправити їх на «свої» пристрої. Таким чином захоплені мережеві пристрої починають працювати як вузли «man-in-the-middle» або «black hole / grey hole».

Це дозволяє злодію маніпулювати вмістом будь-якого пакету, що отримує скомпрометований пристрій. Також зловмисник може успішно зареєструвати "підроблений" контролер в площині управління мережі. За допомогою цього контролера зловмисник може мати можливість впливати на доступність інших контролерів в мережі, змінювати правила, встановлені в кеш-пам'яті та ефективно зупиняти / маніпулювати роботою додатків в площині додатків.

C. Шкідливі додатки. Враховуючи можливість фреймворку SDN інтеграції сторонніх програм, існує проблема встановлення зловмисних програм на контролер. Дії додатків, що показують шкідливу поведінку в межах SDN середовища, можуть мати катастрофічні наслідки.

Додатки, що займаються глибоким аналізом пакетів можуть стати потенційними носіями ризику для мережі - вони можуть бути в змозі опосередковано контролювати всю мережу через інформацію, яку зібрали під час аналізу пакетів.

Збільшений об'єм даних та спосіб, яким він централізовано локалізується є тим, що дає можливість шкідливим програмам загрожувати цілісності та конфіденційності інформації про користувача / мережу.

D. Атаки на площину управління-даних. Ще одне місце SDN, яке дає можливість здійснити атаку – це абстрактне місце між площинами управління та даних. Специфікація OpenFlow передбачає використання TLS (Transport Layer Security) опціонально, що робить цю площину уразливою до безлічі типів атак, таких як man-in-the-middle, black hole тощо.

1) Атака man-in-the-middle: атаки цього типа відбуваються коли скомпрометований мережевий пристрій встановлюється / стоїть між контролером та шляхами передачі даних на площині даних. Замість безпосереднього пересилання повідомлень до контролера (або навпаки), вузол "man-in-the-middle" може маніпулювати / перевіряти вміст пакетів [13].

2) Атака Black hole : атаки такого типу відбуваються, якщо скомпрометований мережевий пристрій встановлюється між пристроєм, на який спрямована атака, і контролером, і просто відклоняє будь-які отримані ним пакети, не пересилаючи їх до контролера. Це призводить до проблем у мережевих комунікаціях та наданні послуг, що становляться недоступними реальним користувачам.

E. Підслуховуючі атаки. Зловмисники, які намагаються отримати незаконний доступ до мереж SDN або зупинити доступність служб, можуть вдаватися до підслуховування трафіку (акт незаконного захоплення та

перевірки пакетів, що передаються через мережу) на певних підключеннях в мережі. Це може дозволити їм зібрати суттєву інформацію, яка потім може бути використана для здійснення більш потужних атак. Атаки з підслуховуванням тривалий час проводилися в традиційних мережевих інфраструктурах - бездротові архітектури особливо вразливі через передачу даних по повітрю. Проте, в контексті SDN, підслуховування можна здійснювати з метою перевірки пакетів на площині управління-даних, а також виключно на площині даних. На площині даних режим "підслуховування", що інтегрований у комутатори OpenFlow, може бути використаний зловмисником, який міг скомпрометувати комутатор, щоб перевірити пакети, передані навколишніми комутаторами. У певному сенсі підслуховування, яке здійснюється на площинах даних та управління, є більш пасивною атакою і не впливає безпосередньо на доступність, конфіденційність чи цілісність даних. Однак, така атака дає змогу зловмисникам здійснювати додаткові атаки на базі зібраних даних.

F. Порівняння типів атак. Нижченаведена таблиця підсумовує наведені вище атаки і дозволяє побачити площини абстракції, які можуть знаходитися під впливом визначених типів атак в SDN-архітектурі, та конкретні аспекти безпеки, які вони потенційно можуть скомпрометувати.

Таблиця 1. Підсумок впливу атак на площини SDN

Тип атаки	**Уразлива площина SDN**	**Вражені аспекти безпеки**		
		Доступність	*Конфіденційність*	*Цілісність*
DDoS	Управління, даних	+		
DoS	Управління, даних	+		
Викрадений / підроблений контролер	Управління, даних, додатків	+	+	+
Шкідливі додатки	Управління, даних		+	+
Man-in-the-middle	Управління, даних, управління-даних		+	+
Black hole	Управління, даних управління-даних	+	+	
Підслуховування	Управління, даних, додатків		+	

Література

1. Jakob Spooner A Review of Solutions for SDN-Exclusive Security Issues // IJACSA // Jakob Spooner, Dr Shao Ying Zhu // Vol. 7, No. 8, 2016. – P. 113-122.
2. “OpenFlow Specification 1.5.1” - Open Networking Foundation, March 15, 2015.