і може бути охарактеризований як система адаптації автогрейдера до змінних умов експлуатації [1].

Експериментальні дослідження показали, що варіювання кутів повороту та нахилу передніх коліс має значний вплив на курсову стійкість. Оптимальні значення цих параметрів встановлюються з урахуванням умов експлуатації, що дозволяє підтримувати стабільність руху автогрейдера в різних умовах [2, 3].

Усі зазначені аспекти вказують на ефективність запропонованого методу та його потенціал у забезпеченні курсової стійкості автогрейдера в різних умовах експлуатації.

Література

1. V Shevchenko, O Chaplyhina, I Pimonov, O Reznikov, S Ponikarovska Mathematical model of a motor-grader movement in the process of performing working operations (IOP Conference Series: Materials Science and Engineering, Dnipro, 2020) doi:10.1088/1757-899X/985/1/012009

2. Shevchenko V., Chaplygina A, Krasnokutsky V., Logvinov E. The analytical research of the dynamic loading effect on the road-holding ability characteristic signs of earth-moving machine // International scientific journal trans & motauto world – Scientific technical union of mechanical engineering industry-4.0, Sofia, Bulgaria, 2018. Vol. 3 (2018), Issue 2. P. 57–61.

3. Shevchenko V. O., Beztsennaya Zh. P., Chaplygina A. M. Methods to determine measures providing a motor-grader road-holding ability // IX International conference for young researchers. Technical sciences. Industrial management. Proceedings. Burgas, Bulgaria, 2015. P. 52–57.

ПРОБЛЕМАТИКА ПОБУДОВИ ПРОГРАМНО-КОНФИГУРОВАННИХ МЕРЕЖ

Плєхова Ганна Анатоліївна, кандидат технічних наук,
доцент, завідувач кафедри інформатики та прикладної математики,
Харківський національний автомобільно-дорожній університет,
e-mail: plehovaanna11@gmail.com, ORCID: 0000-0002-6912-6520
Костікова Марина Володимирівна, кандидат технічних наук, доцент,
e-mail: kmv_topaz@ukr.net, ORCID: 0000-0001-5197-7389
Козачок Лариса Миколаївна, старший викладач кафедри інформатики
та прикладної математики,
Харківський національний автомобільно-дорожній університет,
e-mail: LarisaK2010@ukr.net, ORCID: 0000-0002-5246-4240

Мережева безпека сьогодні займає важливе місце у комплексі засобів підвищення захисту мереж від несанкціонованого втручання. Важливо місто в цьому відводиться мережі SDN. Особисту увагу відводять протоколам марш-рутизації. В свою чергу протоколи потребують системної та скоординованої

взаємодії тому що необхідно одночасно розглядати множини мережних елементів SDN. До таких елементів відносяться SDN-комутатори, контролери мережі які використовуються під час формування (розрахунку) шляхів і правил потоків, вздовж яких має забезпечуватися необхідний рівень безпеки. В свою чергу рівень безпеки встановлюється за обраними показниками або критеріями [1].

В роботі проведено аналіз щодо вразливостей площини даних SDN, розглянуті функціональні можливості засобів маршрутизації протидії можливим атакам, показана перспективність використання засобів безпечної маршрутизації.

Аналіз засобів проведено на основі базових метрик критичності вразливостей, вони в свою чергу використовуються для підвищення рівня мережної безпеки площини даних SDN. Проведено аналіз стандарту CVSS, проаналізований кількісний розрахунок рівня вразливості мережного обладнання, показано доцільність його використання під час розробки та дослідження перс пективних підходів до безпечної маршрутизації у площині даних SDN (Software-Defined Networking, SDN) [1].

Розглянути підходи до проектування та побудови програмно-конфігуровані мережі (Software-Defined Networking, SDN) та їх експлуатації. Основні підходи для інфокомунікаційних мереж базуються на тому, що шляхом розділення площин управління (controlplane) та передавання даних (dataplane) ми досягаємо бажаного ефекту: такий розподіл надає мережі безпосередньої програмованості та динамічності; дозволяє абстрагувати функціональні можливості рівня інфраструктури.

На сьогоднішній день існують різні архітектури. Всі архітектури відокремлюють логіку управління від ресурсів поза пристроєм. Всі підходи до побудови SDN включають контролер і відповідні прикладні програмні інтерфейси – Southbound API та Northbound API.

Віртуалізація мережних функцій (Network Functions Virtualization, NFV) є стандартизованим способом для розробки, впровадження та керування мережними службами. NFV використовує концепцію, яка передбачає заміну спеціальних пристроїв мережної інфраструктури. Проводимо заміну маршрутизаторів та брандмауерів – стандартними серверами, комутаторами, сховищем та хмарою. Можливо навіть використовувати туманну обчислювальну інфраструктуру. NFV відокремлює функції мережі, такі як маршрутизація, комутація та безпека від виділених апаратних пристроїв або пропрієтарних и це дозволяє їм працювати в межах програмного забезпечення.

Використання NFV працює таким чином що головною метою є те, щоб використовувати стандартні технології віртуалізації для консолідації апаратного забезпечення. Крім того це дозволяє проводити віртуалізацію мережних функцій у блоки, які в свою чергу можна об’єднувати для створення наскрізних комунікаційних послуг. Така реалізація можлива для будь-якої функції площини управління або площини даних. Причому можливо використовувати як середовище дротяних мереж так і без дротяних.

NFV складається з трьох основних компонентів. Розглянемо їх більш детально. Перше це віртуалізовані мережні функції (Virtualized Network Functions, VNF). Наступна NFVI – це загальні апаратні та програмні компоненти, де розгортаються VNF функції. Необхідно звернути увагу на середовище керування та оркестровки NFV (Management and Orchestration, MANO).

Згідно з загальними вимогами для забезпечення безпеки об'єкта необхідно забезпечити п'ять основних функцій безпеки CIAAA [2]: конфіденційність (Confidentiality); цілісність (Integrity); доступність (Availability); антентичність (Authenticity); підзвітність (Accountability).

Розглянемо кожну окремо. Спочатку конфіденційність – вона забезпечує конфіденційність інформації про дані або осіб. За допомогою цієї функції інформація не розголошується не авторизованим користувачам. Цілісність надає гарантії, що інформація та передбачувана робота системи не будуть випадково чи навмисно змінені неавторизованими користувачами. Наступна функція – доступність. Вона гарантує, що неавторизовані користувачі не зможуть отримати доступ до систем і послуг. Що стосується автентичності, то вона гарантує, що користувачів можна перевірити та довіряти їм. Після перевірки система довіряє користувачам як таким, ким вони себе видають и дозволяє використовувати всі вхідні дані (вважається, що вони надходять до системи з надійного джерела). Розглянемо також підзвітність. Підзвітність породжує вимогу, щоб дії суб'єкта відстежувалися виключно щодо цього суб'єкта.

Розглянемо систему, організацію або кіберпростір, який складається з трьох ключових елементів. Спочатку це реальні та віртуальні об'єкти (сутності), наступні – інфраструктура взаємозв'язку (комунікацій) та останні – взаємодія між об'єктами через інфраструктуру.

Більш детально зупинімось на кожному пункті, розглянув реальні та віртуальні сутності, які складаються з реальних об'єктів та фізичних пристроїв. Прикладом можуть бути люди (користувачі систем), також комп'ютери, датчики, мобільні телефони, програмне забезпечення та послуги, електронні пристрої.

Важливим етапом організації є інфраструктура. Вона включає мережі, інформаційні системи та сховища, бази даних які з'єднують і підтримують об'єкти в системі/просторі. Цей елемент організує взаємодію, яка охоплює дії та взаємозалежності між об'єктами системи/кіберпростору.

Таким чином інформаційну або кібербезпеку вважаємо процесами, практиками, системами, інструментами, концепціями та стратегіями для запобігання та захисту кіберпростору від несанкціонованої взаємодії. Тобто для агентів і елементами простору для підтримки та збереження конфіденційності, цілісності, доступності та інших властивостей простору та його ресурсів, що потребують захисту. Кібербезпека пов'язана з виявленням вразливостей кіберпростору. Вона проводить оцінку ризику, пов'язаного із загрозами, які використовують вразливість системи, і крім того надає рішення для безпеки. Враховуючи вразливість безпеки, тобто слабку сторону в системі (компонент/ продукт/система/ кіберпростір), таку яка може дозволити зловмиснику скомпрометувати

конфіденційність, цілісність, доступність, автентичність або підзвітність цієї системи.

Використовуючи термін загрози та ризики необхідно враховувати, що вони тісно пов'язані, але не рівнозначні. Будь-яка сутність, дія чи стан – є загроза, якщо вони приводять до шкоди, втрат, пошкодження та/або погіршення існуючих умов. Термін ризик – пов'язаний із загрозою, є характеристикою, яка охоплює: вплив або важливість інциденту загрози; ймовірність або потенціал інциденту загрози в майбутньому; потенційні втрати (збитки) через інцидент загрози.

Оцінка ризику, пов'язаного із загрозою, сприяє розробці нових рішень щодо безпеки та формулюванню вимог до цих рішень [2].

Оскільки мережні компоненти віртуалізовані, NFV-мережі містять рівень абстракції, якого немає в традиційних мережах. Захист цього складного та динамічного середовища, яке охоплює віртуальні та фізичні ресурси, елементи керування, протоколи, а також границі між віртуальними та фізичними мережами, є складним завданням з багатьох причин:

1) Залежності гіпервізора: Гіпервізори доступні від багатьох постачальників. Вони повинні усунути вразливі місця безпеки у підконтрольному програмному забезпеченні. Розуміння базової архітектури, розгортання відповідних типів шифрування та ретельне застосування виправлень є критичними для безпеки гіпервізорів.

2) Еластичні границі мережі: У NFV мережна структура (fabric) виконує численну кількість функцій. Фізичні та віртуальні границі розмиті або відсутні в архітектурі NFV, що ускладнює проектування систем безпеки.

3) Динамічні робочі навантаження: Хоча NFV пропонує гнучкість і динамічні можливості, традиційні моделі безпеки є статичними і не можуть розвиватися, коли топологія мережі змінюється відповідно до вимог.

4) Додавання сервісів і служб: NFV надає еластичні, прозорі мережі, оскільки структура (fabric) інтелектуально маршрутизує пакети, які відповідають критеріям, що можуть налаштовуватись. Традиційні елементи керування безпекою розгортаються логічно та фізично. У NFV часто буває відсутня так звана точка додавання для служб безпеки, які ще не розміщені на гіпервізори.

5) Перевірка зі збереженням стану (stateful)/без збереження стану (stateless): Операції безпеки протягом останнього десятиліття ґрунтувалися на передумові, що перевірка зі збереженням стану є більш досконалою ніж без збереження стану. Проте NFV може додати складності, коли засоби контролю безпеки не можуть впоратися з асиметричними потоками, створеними кількома дублюючими мережними шляхами та пристроями.

6) Масштабованість доступних ресурсів: Технології глибокої перевірки, наприклад, брандмауери наступного покоління та дешифрування у межах протоколу безпеки транспортного рівня (TLS), потребують ресурсів і не завжди масштабуються без можливості розвантаження.

Група експертів з безпеки ETSI, яка концентрує зусилля на безпеці архітектури програмного забезпечення, визначила потенційні вразливі місця

безпеки NFV і встановила, чи є вони новими проблемами чи просто існуючими проблемами в різних формах і проявах [2].

Нижче наведено нові проблеми безпеки, пов’язані з NFV:

– перевірка та забезпечення дотримання топології;

– наявність інфраструктури підтримки управління;

– безпечне початкове завантаження;

– безпечний збій; ізоляція продуктивності;

– автентифікація, авторизація та облік користувача/клієнта;

– послуги часу автентифікації;

– приватні ключі в клонованих образах;

– методи обходу стандартних процедур автентифікації, несанкціонований віддалений доступ через віртуалізовані функції тестування та моніторингу; ізоляція кількох адміністраторів.

Висновки

Таким чином, SDN представляє собою нову мережну парадигму, а її вплив полягає у формі нової структури, нових компонентів, структурних рівнів та інтерфейсів. SDN несе з собою нові виклики безпеці, які виходять за рамки традиційних мереж. Оскільки SDN відокремлює рівень керування від рівня даних, ця технологія приносить із собою нові набори компонентів, інтерфейсів, а також багато нових питань безпеки.

Література

1. Плєхова Г. А., Костікова М. В. Актуальні проблеми інформаційної безпеки. *Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті* : матеріали Всеукраїнської науково-практичної Internet-конференції (Харків, 15–16 листопада 2022 р.). Харків, 2022. С. 68–73. URL: https://rcf.khadi.kharkov.ua/fileadmin/F-HIGHWAY/Інформатики_і_прикладної_математики/Матеріали_ Всеукр.конф._2022_-1-ред.pdf.

2. Liu Y., Zhao B., Zhao P., Fan P., Liu H. A survey: Typical security issues of software-defined networking. *China Communications*. 2019. No. 16 (7). pp. 13–31. DOI: https://doi.org/10.23919/JCC.2019.07.002.