SECTION: TELECOMMUNICATIONS AND RADIO ELECTRONICS.

SEKCJA: TELEKOMUNIKACJA I ELEKTRONIKA RADIOWA.

How to cite: Faychuk, V. (2023). Research of routing models taking into account information security risks. *Global Innovations and Collaborative Solutions in Contemporary Science* (pp. 344-348). Futurity Research Publishing. https://futurity-publishing.com/international_conference_3

Research of routing models taking into account information security risks

Файчук Валентин Олександрович [1]

[1] *магістр, студент аспірантури, кафедра телекомунікацій, Інститут телекомунікацій радіоелектроніки та електронної техніки, Національний університет «Львівська політехніка», м. Львів , Україна, faitchouk.valentyn@gmail.com, https://orcid.org/0000-0002-8779-6595*

Accepted: December 9, 2023 | **Published**: December 14, 2023 | **Language:** Ukrainian

Abstract: This abstract explores a secure routing flow model in a software-defined network using a vulnerability catalog. The purpose of this paper is to analyze the capabilities of routing tools to counter potential attacks and the prospects for using SDN data planes, taking into account key indicators of materiality to increase the level of network security. The methods of analysis, information gathering, and generalization were used for the theoretical development of the topic. In the main results, by changing the route metric, it is recommended to improve the existing secure routing model by taking into account the key vulnerability importance metric.

Keywords: global routing model, risk assessment, cyber security.

Вступ

Дотепер гарантія стабільності кіберпростору і безпеки телекомунікацій є важливим і актуальним питанням, особливо в контексті інтенсивної цифрової трансформації. На превеликий жаль, існуюча телекомунікаційна мережа не відповідає вимогам сучасності і постійно зростаючим потребам користувачів інформаційних сервісів і сервісних послуг. Для вирішення цього важливого завдання, перед обличчям атак зловмисників, порушення цілісності мережевих елементів, збоїв різного походження, перевантаження мережі, сучасна ТСМ забезпечує і підтримує прийнятний

рівень обслуговування, адаптивно реагує на всі ці інциденти, захищаючи критично важливі мережеві елементи і їх компоненти, обмежуючи зокрема негативний вплив на мережу. На сучасному етапі численна кількість дослідників вивчали питання моделей анонімної маршрутизації, досліджуючи їхню ефективність та можливість застосування в контексті забезпечення конфіденційності та безпеки у мережевих комунікаціях. До прикладу, Єременко та Плєхова (2022) розглядають модель безпечного потоку маршрутизації, яка ґрунтується на ключових показниках вразливості в програмно визначених мережах. Автори ретельно вивчають та аналізують цю модель з метою подальшого вдосконалення підходів до забезпечення безпеки в мережевих структурах, враховуючи актуальні вимоги та виклики сучасності.

Аналіз можливостей засобів маршрутизації для боротьби з можливими атаками підтвердив перспективи використання площин даних SDN з урахуванням ключових показників важливості вразливостей для підвищення рівня мережевої безпеки.

У свою чергу, Evdokymenko et al. (2020) пропонують вдосконалену модель маршрутизації потоків, яка враховує ризики інформаційної безпеки, використовуючи ключові показники тяжкості вразливості. Підхід, застосований до концепції електронних доказів у кримінально-процесуальному кодексі та інших розділах внутрішнього процесуального права аналізують (Кобець & Кобець, 2022).

Лемешко та ін. (2022) розглянули моделі та методи маршрутизації в інформаційно-комунікаційних мережах. Автори визначили, що теоретичною основою для перспективних протоколів маршрутизації та технічних засобів традиційного та програмно налаштованого управління трафіком. Таким чином, на кожному рівні моделі OSI існує безліч одночасних аналізаторів трафіку, VPN (віртуальних приватних мереж), брандмауерів і систем виявлення і протидії атакам, які можуть бути використані для підвищення безпеки ТСМ як на кожному рівні системи, так і по всій мережі. До того ж, особливу увагу слід приділити тому, як забезпечити захист ТСМ, використовуваного на мережевому рівні. Також, використання протоколу безпечної маршрутизації в ІТ має бути ізольованим. Завдяки РВМ можна не тільки підвищити безпеку ТСМ, але і забезпечити кіберстійкість мережі.

Результати дослідження

Головною ідеєю в основі безпечної маршрутизації є підвищення кіберстійкості та безпеки. Для підвищення відмовостійкості і стійкості до кіберпростору все частіше використовуються протоколи швидкої маршрутизації, які в основному є реактивними і орієнтовані на захист мережевих елементів, таких як вузли, канали зв'язку і маршрути. Втім, незважаючи на те, що ТКМ є більш ефективним з точки зору підвищення своєї безпеки порівняно з проактивним ПБМ, реактивні протоколи втрачаються з точки зору якості обслуговування ТКМ і, перш за все, середньої затримки мережі. Це пов'язано з тим, що в першу чергу необхідно оцінити стан безпеки мережі та її елементів на основі аналізу параметрів безпеки і, при необхідності, розрахувати маршрут з використанням цих параметрів. Nizovtsev & Parfylo (2023) описали можливість використання маршрутизаторів Wi-Fi для встановлення мобільних терміналів, а також їх мережеву активність під час розслідування кіберзлочинності. Самойленко (2020) детально охарактеризувала основи методології розслідування злочинів, скоєних у кіберпросторі. Авторка розглядає елементи криміналістичних характеристик злочину, які визначаються деталями кіберпростору як місця злочину. У монографії звернено увагу на проблемні аспекти порушення кримінальної справи, визначено деталі використання приватної інформації при розслідуванні злочинів, вчинених у кіберпросторі, подано ситуацію розслідування та тактичне функціонування її розслідувань (Самойленко, 2020).

Собчук та ін. (2021) пропонують вдосконалений алгоритм маршрутизації для самоорганізованих інформаційних мереж. Його особливості полягають в тому, щоб зменшити надмірність потоку керуючих сигналів в мережі, передаючи функцію вибору маршруту всіх ретрансляційних вузлів, забезпечуючи швидку адаптацію і самовідновлення мережі по альтернативних маршрутах у випадку відмови активних ретрансляційних вузлів. Тиртишніков та ін. (2017) розглянули особливості апаратної реалізації оптимального алгоритму адаптивної маршрутизації повідомлень на основі координат у різних мережах тороїдальної мережі зв'язку.

Zubok (2019) визначив, що один із найважливіших кроків при моделюванні впливу атаки на маршрутизацію є створення офіційної глобальної моделі маршрутизації через Інтернет. На основі проведеного аналізу ПБМ слід зазначити, що всі вони є вдосконаленнями порівняно з традиційними протоколами маршрутизації, що використовують показники безпеки. Подальші вдосконалення протоколу та моделі безпечної маршрутизації для усунення недоліків існуючих рішень повинні відповідати наступним вимогам:

- аналіз особливостей структурно-функціональної будови ТКМ;
- підтримка потокової передачі різних типів трафіку;
- врахування параметрів безпеки як окремих елементів, так і всієї мережі;
- розгляд ризиків інформаційної безпеки на основі існуючих та виявлених вразливостей у мережевих елементах;
- підтримка рекомендованих показників якості обслуговування;
- прийнятна обчислювальна складність і масштабованість кінцевого рішення за умови більшої реалізації протоколу.

Таким чином, у цьому дослідженні було вирішено нагальну проблему вдосконалення моделі маршрутизації потоків з урахуванням ризику інформаційної безпеки за допомогою базового індексу тяжкості вразливості.

Удосконалення моделі полягає у введенні вагового коефіцієнта в якості метрики маршруту, який характеризує ризики, створювані вразливістю, виявленими в вузлах ТКМ, і вимірює умовну вартість використання каналів зв'язку. Використання цих коефіцієнтів в рамках моделі маршрутизації потоків гарантує, що потоки пакетів передаються по найбільш безпечному маршруту в ТКМ. У цей час мережа покладається на практичні реактивні механізми для захисту від крадіжки префіксів. Це пояснюється тим, що запропоновані проактивні механізми повністю ефективні лише при глобальному розгортанні, і оператори неохоче впроваджують їх через пов'язані з цим технічні та фінансові витрати. Захист від крадіжки складається з 2 етапів: виявлення і пом'якшення наслідків. Аналіз механізму атаки, в залежності від її мети і варіантів її реалізації. Виявлення в першу чергу забезпечується сторонніми службами, такими як bgpmon, який відстежує фактичний маршрут, повідомляючи адміністраторів мережі про підозрілі події, пов'язані з префіксом на основі на основі інформації про маршрут, а також шляхом відстеження та моніторингу оновлень оголошень про маршрути BGP. Якщо трапиться інцидент, уражена мережа вживатиме заходів для пом'якшення наслідків цієї події, наприклад, оголосить більш конкретний префікс для мережі або зв'яжеться з іншими користувачами, щоб виключити підроблену рекламу. Втім через поєднання технічних і практичних проблем з розгортанням існуючий підхід реагування в значній мірі неадекватний. Зокрема, при використанні найсучасніших технологій виникають наступні основні проблеми: різні типи маршрутизаційних атак, комбінація методів призводить до того, що не існує надійного способу виявити перехоплення маршруту. Оператор повинен

заздалегідь повідомляти про будь-які законні зміни в політиці маршрутизації (формування нових взаємодій між ASS, оголошення нових префіксів та ін.). Необхідно переконатися, що такі зміни не розглядаються як підозрілі події в системі виявлення атак з боку умовних третіх осіб, у свою чергу, прийняття менш суворої політики компенсації нестачі оновленої інформації і зниження навантаження. І, згідно з поточною практикою, швидкість реагування на інциденти в будь-якому випадку буде нижчою, оскільки попередження від систем моніторингу та сторонніх сервісів доведеться перевіряти вручну. В процесі оцінки ризиків описуються особливі вимоги до якості інформаці, тобто максимально можливий рівень повноти, точності та відповідності вимогам на момент отримання та якості її джерел.

Висновки

Отже, важливим визначенням ризику є прогнозування можливого результату атаки та оцінка масштабів цього впливу. Зокрема, висвітлено необхідність врахування маршруту поширення, зони впливу та кількості «пошкоджених» маршрутів. Однією з ключових рекомендацій для забезпечення ефективної оцінки ризику є надання офіційного опису об'єктів глобальної маршрутизації та взаємозв'язків між автономними системами. Останнє сприяє можливості отримати повний і чіткий зоровий образ структури, що дозволяє більш точно прогнозувати можливі наслідки атаки. Ці кроки є важливими кроками для моделювання кібератак на глобальну маршрутизацію, формулюючи завдання управління ризиком перехоплення маршрутів конкретним вузлом як завдання пошуку найбільш ефективної топології зв'язку. Зазначений у тексті формальний опис двох компонентів процесу маршрутизації – префікса IP і розрахунку вибору шляху – є значущим етапом у створенні бази для аналізу та виявлення слабких місць системи. Ця деталізація дозволяє ефективно аналізувати потенційні вразливості та розробляти стратегії захисту, спрямовані на запобігання можливим загрозам. Отже, проведений аналіз, представлений вище, має потенціал для оптимізації методів оцінки ризику глобальної маршрутизації. Останнє може бути досягнуто через узагальнення та врахування офіційного опису та конкретизацію компонентів маршрутизації, що сприятиме більш ефективному управлінню та захисту мережевої інфраструктури.

Література

Єременко, О. С., & Плєхова, Г. А. (2022). Дослідження моделей безпечної маршрутизації на основі базових метрик уразливостей в мережах SDN. *Проблеми телекомунікацій*, (2 (31)), 34-50. https://doi.org/10.30837/pt.2022.2.03

Кобець, М. В., & Кобець, Р. М. (2022). Використання можливостей wi-fi роутерів під час виявлення та розслідування кримінальних правопорушень. *Криміналістичний вісник*, *38*(2), 36–47. https://doi.org/10.37025/1992-4437/2022-38-2-36

Лемешко О.В., Єременко О.С., Євдокименко М.О., Шаповалова А.С., Слейман Б. (2022). *Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах.* Харків: ХНУРЕ.
Одеса :ТЕС.
Самойленко, О. А. (2020). *Основи методики розслідування злочинів, вчинених у кіберпросторі*.
Собчук В.В., Бреславський В.О., Лаптєв С.О., Лаптєва Т.О., Загиней А.Ю., & Коваленко О.В. (2021). Розробка алгоритму маршрутізації самоорганізованих інформаційних джерел. *Deutsche Internationale Zeitschrift für zeitgenössische Wissenschaft,* (*7-1*), 32-37. doi: 10.24412/2701-8369-2021-7-1-32-37

Тиртишніков, О.І., Курчанов, В.М., Мавріна, М.О.& Кор, Ю.М. (2017). Особливості апаратної маршрутизації у тороїдально-решітчастих комунікаційних мережах Системи управління, навігації та зв'язку, 2 (42), 150-153. http://journals.nupp.edu.ua/sunz/article/view/690

Evdokymenko, M., Shapovalova, A., & Shapovalov, M. (2020). Flow model of routing taking into accountinformation security risks using basic vulnerability criticality metrics.*Electronic scientific publication - "Telecommunications Problems" magazine, 1 (26),* 48-62. https://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf

Nizovtsev, Y., & Parfylo, O. (2023). Using the wi-fi capabilities of routers for determining a mobile terminal and its network activity during cyber crimes investigation. *Information and law,* (4(47)), 124–135. https://doi.org/10.37750/2616-6798.2023.4(47).291614

Zubok, V. (2019). A formal description of objects and processes of global routing on the Internet to assess the impact of cyberattacks on routing. *Registration, storageand processing of data, 4,* 67-75. http://drsp.ipri.kiev.ua/article/download/199409/199726