DOI: 10.36910/6775-2524-0560-2020-39-20
УДК: 004.7
Войтенко Єлизавета Дмитрівна, магістрант.
Орлова Марія Миколаївна, к.т.н., доцент.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна.

АНАЛІЗ ВРАЗЛИВОСТІ БЕЗПЕКИ ФУНКЦІОНУВАННЯ BGP ТА ПРИЧИН СКЛАДНОСТІ БОРОТЬБИ З НИМИ

Войтенко Є. Д., Орлова М. М. Аналіз вразливості безпеки функціонування BGP та причин складності боротьби з ними. У цій статті проведено дослідження та аналіз вразливостей роботи BGP зі сторони його алгоритмічної поведінки та зі сторони механіки налагоджування зв'язку між автономними системами за вимогами даного протоколу. Також наведений системний аналіз проблематики введення схвалених IETF розширень до цього протоколу, проблематика тестування нових рішень, а також причин повної або часткової відмови від остаточного їх загальнодоступного використання. На основі виконаного аналізу описані можливі варіанти подальших напрямків дій для боротьби з описаними вразливостями.
Ключові слова: Border Gateway Protocol, BGPSEC, безпека маршрутизації, безпека Інтернету, міждоменна маршрутизація.

Войтенко Е. Д., Орлова М. Н. Анализ уязвимости безопасности функционирования BGP и причин сложности борьбы с ними. В этой статье проведено исследование и анализ уязвимостей работы BGP со стороны его алгоритмической поведения и со стороны механики налаживания связи между автономными системами согласно требованиям данного протокола. Также приведен системный анализ проблематики введения одобренных IETF расширений к этому протоколу, проблематика тестирования новых решений, а также причин полного или частичного отказа от окончательного их общедоступного использования. На основе выполненного анализа описаны возможные варианты дальнейших направлений действий для борьбы с описанными уязвимостями.
Ключевый слова: Border Gateway Protocol, BGPSEC, безопасность маршрутизации, безопасность Интернета, междоменная маршрутизация.

Voitenko I., Orlova M. Analysis of the security vulnerability of BGP functioning and the reasons for complexity of dealing with them. This article investigates and analyzes the vulnerabilities of BGP from its algorithmic behavior and from the mechanics of debugging autonomous systems according to the requirements of this protocol. It also provides a systematic analysis of the issue of the introduction of approved IETF extensions to this protocol, the issues of testing new solutions, as well as the reasons for the total or partial rejection of their final public use. Based on the analysis, possible options for further action to address the described vulnerabilities are described.
Keywords: Border Gateway Protocol, BGPSEC, routing security, Internet security, cross-domain routing.

Постановка наукової проблеми. У світі сучасних комунікацій чималу роль відіграє протокол граничного шлюзу BGP (Border Gateway Protocol). Саме цей протокол є засобом междоменної маршрутизації, що об'єднує Інтернет, забезпечуючи маршрут передачі IP-пакетів для обміну між мережами, керованими різними провайдерами, по всьому світу.

І хоча перша версія протоколу побачила світ у далекому 1989 році, а значить і всі недоліки у внутрішніх механізмах його безпеки відомі теж вже досить немалий час, протокол BGP досі залишається вразливим для безлічі атак, які можуть викликати великомасштабні збої в роботі, стати причиною витоку маршрутів, а також можуть бути використані для інших шкідливих цілей в глобальній мережі, таких як розсилка спаму або відстеження трафіку. Наприклад, в 2014 році викрадення маршрутів BGP було вдало використано для крадіжки понад 83 тисяч доларів в криптовалютному еквіваленті [1, с. 387]. Таким чином, забезпечення безпеки BGP є ключем до підвищення загальної безпеки екосистеми Інтернету.

Знаючи все це здається дивним відсутність постійного активного вдосконалення політики безпеки маршрутизації в BGP, адже забезпечення надійності комутації в комп'ютерних мережах постійно актуальний та досить популярний напрямок для роботи серед спеціалістів та науковців. Насправді вся ця бездіяльність лише зовнішня. Інженерна рада Інтернету IETF (Internet Engineering Task Force) – відкрите міжнародне співтовариство проектувальників, учених, мережевих операторів і провайдерів, постійно знаходиться в пошуку рішень, але лише 17 з усіх, що коли-небудь були надіслані на розгляд, були затверджені та мали спробу виведення реалізації для широкого доступу [3]. Отже, такий малий об'єм впровадження має під собою досить серйозне підґрунтя у вигляді складності впровадження змін до BGP через обмеженість рівня втручання зі сторони багатьох аспектів.

Аналіз останніх досліджень і публікацій. Пропозиції з приводу забезпечення безпеки BGP надходять не тільки від IETF [1-4], але і від промислових діячів, а також від академічної спільноти [5]. Попередні опубліковані дослідження дослідницької спільноти з усього світу були сфокусовані саме на оцінці продуктивності та ефективності пропозицій щодо безпеки [5, 6], їх обмежень та переваг щодо їх гарантій безпеки [7], методів, які використовуються для захисту BGP [7], динаміки їх архітектури [8] і аналіз їх додаткових переваг безпеки при впровадженні та повноцінне функціонування [8].

Постановка завдання. Метою статті є дослідження вразливостей безпеки в BGP, їх класифікація, системний аналіз причин відсутності повноцінно працюючих рішень, причин відмов від пропозицій з вирішення даної проблеми та складностей використання навіть затверджених рішень.

Виклад основного матеріалу дослідження. З накопиченням практичного досвіду роботи з BGP-4 зросла обізнаність про його недоліки та слабкі місця. Основним аспектом безпеки, обговорюваним і найбільш виділеним, підкресленим в Заявці на обговорення RFC (Request for Comments) BGP, інформаційному документі, що містить технічні специфікації та стандарти Інтернету в цілому та BGP вчасності, є доступність. Існує розуміння того, що BGP, як єдиний інструмент маршрутизації між автономними системами, повинен забезпечувати якомога більшу доступність, в тому числі і в разі атаки або ж ненавмисного збою.

Отже, за таких вимог для підвищення доступності більшість розширень протоколу BGP повинні бути, та власне вже в основному і є, націлені на зниження складності управління та ручного налаштування оголошувачів маршрутних таблиць BGP, які найбільш схильні до ненавмисних збоїв, а також на зменшення нестабільності маршрутизації, з огляду на зростаючу складність топологій мереж та політик розсилки.

Іншими ж аспектами безпеки, тема яких піднімається в RFC, можна назвати цілісність та правильність інформації щодо маршрутизації. Вони обговорюються в документаціях спеціально присвячених саме вразливостям безпеки конкретно BGP або протоколів маршрутизації загалом. Докладний аналіз уразливості протоколу BGP був опублікований в 2006 році [2]. Хоча в документі, в основному, розглядаються вразливості, пов'язані з механізмами якраз сеансів BGP та обміну повідомленнями, також в ньому згадується, що вразливості, пов'язані саме з алгоритмічною поведінкою BGP. Конкретні причини в тому документі ще не були повністю сформовані. Однак зараз можна сказати, що існує три наступні групи «відсутностей», які впливають на роботу протоколу.

1. Відсутність аутентифікації повідомлень BGP, що не забезпечують цілісність, аутентифікацію та динамічну перевірку даних BGP в повідомленнях BGP: повідомлення BGP можуть бути підроблені, змінені, видалені або ретрансльовані випадково вузлом чи навіть навмисно сторонньою особою.
2. Відсутність перевірки повноважень мережевих (префіксних) оголошень: будь-який BGP-оголошувач може оголосити маршрут до будь-якого префіксу.
3. Відсутність перевірки аутентичності шляху автономної системи і атрибутів шляху: сам шлях і його окремі атрибути можуть бути змінені під час стрибків оголошення.

Дійсно, коли BGP-приймач отримує BGP-повідомлення, він без якихось додаткових підтверджень вважає, що повідомлення приходить від легітимного партнера, якщо ідентифікаційна інформація в повідомленні просто збігається з інформацією відомого партнера. Крім того, якщо оголошувач BGP обробляє інформацію про маршрутизації, він вважає, що префікси маршрутів в повідомленні були оголошені законно, і що всі автономні системи на маршруті оголошення правильно додали свій власний унікальний номер до маршруту та змінили атрибути шляху без внесення помилкових даних. Як зафіксовано в RFC 4360, «оператор (мережа), який покладається на інформацію, передану в BGP, повинен мати транзитивні довірчі відносини на шляху назад до джерела інформації» [2]. Втім, як правило, це не так, і оскільки все більше мереж підключається до Інтернету, це стає все важче.

Протокол BGP не містить всередині себе жодного механізму для перевірки коректності відправки інформації щодо керівних принципів та норм Інтернет-спільноти. Інтернет складається з взаємозв'язаних мереж. З іншої ж сторони, існує досить чітка ієрархія організацій, які займаються розподілом та делегуванням IP-адрес (номерних ресурсів Інтернету). Управління з присвоєння номерів в Інтернеті IANA (Internet Assigned Numbers Authority) знаходиться на вершині процесу розподілу адрес та розподіляє великі частини простору IP-адрес для IPv4 й IPv6 серед п'яти регіональних реєстрів Інтернету RIR (Regional Internet Registries), що охоплюють різні географічні регіони: ARIN для Північної Америки, LACNIC для Південної Америки та Карибського басейну, RIPE для Європи та Близького Сходу, APNIC

для Азіатсько-Тихоокеанського регіону та AFRINIC для Африки. Ці регіональні реєстри потім виділяють менші пули IP-адрес локальним інтернет-реєстрам LIR (Local Internet Registries) або безпосередньо постачальникам інтернет-послуг ISP (Internet Service Providers). LIR та ISP, в свою чергу, делегують IP-адреси іншим (меншим) інтернет-провайдерам та мережам. Тобто, більшість законних префіксів IP-мережі, які були законно виділені, дотримувалися певного шляху розподілу в ієрархії.

Крім вразливостей, описаних вище, існують вектори атак, пов'язані з механікою зв'язку BGP. Їх можна розділити на три наступні основні категорії.

1. Уразливості, пов'язані з повідомленнями BGP та кінцевим автоматом: існує безліч способів, якими повідомлення BGP може в кінцевому підсумку закрити сеанс BGP, ініціюючи видалення інформації про маршрутизацію, отриманої вузлами BGP.
2. Уразливості, пов'язані з безпекою транспортного рівня: враховуючи, що протокол BGP працює поверх TCP, він успадковує уразливості TCP, оскільки механізм безпеки транспортного рівня не використовується.
3. Уразливості, пов'язані з інфраструктурою, в якій працює протокол BGP: конфігурація, експлуатація та управління інфраструктурою, що підтримує BGP, можуть вплинути на правильну роботу BGP.

Основні мотиви, якими керуються пропозиції щодо безпеки BGP, які були затверджені IETF, суттєво відрізняються між собою, хоча здається, що перелік вразливостей можна звести до чітко розмежованих груп, але при їх вирішенні все знову змішується разом в єдине ціле. Мотиви дуже різняться, від необхідності захисту зв'язку BGP до розвитку фактично з нуля захищених моніторів для перевірки правильності роботи динаміків BGP, основні причини, через які розробники розширень вважали ці рішення хорошим, дуже різноманітні. Це, мабуть, випливало з того, що між цими пропозиціями не існує згоди щодо того, що потрібно забезпечити, яким чином воно має бути захищеним чи які є прийнятні компроміси. Деякі рішення, такі як Listen and Whisper [15], та використання списків вихідних даних стосуються лише суперечливих маршрутів, в той час, коли інші рішення стосуються всіх оголошень маршруту [14].

Крім того, є чіткий вплив перших пропозицій на останні рішення. Багато хто бере елементи першої пропозиції, вдосконалює деякі аспекти або чітко виступає проти якогось принципу та базуючись на цьому пропонує альтернативу. Наприклад, S-BGP [6] запропонував ієрархічну інфраструктуру PKI для перевірки розподілу префіксу IP, до якої пізніше також були включені інші рішення. Однак soBGP [6] запропонував більш децентралізовану структуру PKI з невеликою групою довірених організацій вгорі. А вже потім ESM [6] запропонував ще більш децентралізовану структуру PKI, де кожна автономна система видаватиме власні сертифікати, і лише у випадку конфлікту потрібно буде отримати цей сертифікат.

Крім того, оскільки зазвичай мотивація дизайнерів керується однією особливістю пропозиції рішення та охоплює більше аспектів безпеки BGP, розробник використовує елементи попередніх пропозицій чи іншого вже стандартизованого протоколу. Наприклад, розробники SPV [8] зосередилися на розробці більш ефективного механізму перевірки AS Path, ніж у S-BGP, але використовують централізовану інфраструктуру PKI на зразок S-BGP для перевірки походження префікса.

Нарешті, жодна з цих пропозицій не була повністю реалізована або використана, і лише невелика частина з них досі обговорюється в роботах, пов'язаних з безпекою BGP. Однак багато з цих робіт вплинули на розвиток безпечної та коректної маршрутизації між доменами SIDR (Secure Inter-Domain Routing), а деякі потенційно можуть вплинути на поточні послуги з моніторингу BGP, або Інтернет-провайдерами, або іншими організаціями.

З вивчення життєвого циклу розширень BGP видно, що жодна пропозиція щодо безпеки не була швидко реалізована та розгорнута, незалежно від її мотивації та розробки. Рішення, орієнтовані на безпеку на транспортному рівні, є чудовим прикладом: застарілий TCP-MD5 [12] досі використовується, а TCP-AO та GTSM [13] мають обмежене використання, хоча вони були стандартизовані відповідно 9 та 15 років тому. Навіть для TCP-MD5 пройшло майже десятиліття, щоб вийти за рамки обмеженого тестового використання.

Крім того, основна мотивація та розвиток розробок свідчать про відсутність згоди щодо того, що потрібно забезпечити та що забезпечити в контексті BGP. Деякі пропозиції стосуються забезпечення безпеки в окремих випадках, наприклад, коли існує конфлікт між двома маршрутами, тоді як інші охоплюють усі можливі випадки. Крім того, деякі пропозиції визначали перевірку походження префікса як таку, що стосується сертифіката та атестації розподілу блоку IP-адрес та авторизації транзиту, тоді як

інші визначали це щодо власного оголошення ресурсів або консенсусу Інтернет-провайдерів серед того, що Інтернет-провайдери вважають правильними. Це пов'язано з делегуванням довіри, що має на увазі різні пропозиції та їх залишкові вразливості.

Насправді проблематика визначеності меж в даному питанні дуже значна. Немає згоди за жодним питанням. Від впливу вразливостей одна на одну до того, що вважати вразливостями, а що прийнятними збоями, від того яким способом розподіляти номери автономних систем до того яку частину інфраструктури робити відкритою і так далі.

З іншого боку, якщо відкинути невизначеність головної мети, все одно залишається питання часу на тестування, яке насправді дуже значне і важливе. Спочатку кожне рішення не один раз тестується на тестових імітаційних моделях загального використання та специфічно розроблених. Після цього йде період обмеженого використання, коли розширення випробовують на робочій, проте замкнутій або ж обмеженій, мережі. І, як згадувалося раніше, такий випробувальний термін може тривати роками і в кінці кінців тестове розширення може втратити свою актуальність ще до повноцінного схвалення. На жаль, зменшити випробування за часом і випустити в загальний доступ не ідеально перевірений варіант призводить до завеликої небезпеки у випадку протоколу маршрутизації BGP і даний аспект складності поки що не вдалося зменшити.

А останньою причиною дуже рідкого впровадження пропозицій, щодо покращення безпеки BGP, можна назвати їх вартість. Всі рішення передбачають певний рівень модифікації конфігурації оголошувача маршрутів BGP або використовують пристрої, які діють як проксі, що потребують розширеної конфігурації, збільшуючи ризик потенційних помилок конфігурації, що впливають на доступність. І всі ці витрати лягають на плечі операторів мережі. Закономірним буде питання, а чи зобов'язані оператори мережі та Інтернет-провайдери забезпечувати безпеку маршрутизації? Адже є й інші способи підвищення безпеки, наприклад, моніторинг інформації про маршрутизацію BGP, який можна забезпечити самостійно або ж через спеціалізовані аутсорсингові компаній, такі як ThousandEyes.

Як варіант тимчасового виходу для користувачів, яким безпека потрібна зараз, а не коли знайдуть ідеальне рішення, можна запропонувати захищену маршрутизацію в якості додаткової послуги від провайдерів та мережевих операторів за окремі додаткові витрати. Клієнти, які хочуть покращити гарантії безпеки для трафіку до мережі та з неї, можуть домовитися з провайдером про додатковий рівень безпеки для маршрутизації їх повідомлень та потоків. Провайдери провайдерів та мережеві оператори передають це, дотримуючись усіх кращих практик безпеки оперативної безпеки BGP [14] та конкретно відстежуючи маршрути для цих клієнтів. У цьому випадку зусилля щодо захисту ISP були б досить вузькими, обмежуючи помилки неправильної конфігурації. Крім того, додаткові витрати, понесені провайдером, безпосередньо переносилися б на клієнтів.

Якщо безпечна маршрутизація не є обов'язковою функцією мережевих операторів, клієнтам доведеться платити за забезпечення маршрутизації, чого вони, можливо, не бажають робити. Положення може стимулювати клієнтів, що надають критичні послуги кінцевому користувачу, який працює з публічним Інтернетом, наприклад, Інтернет-банкінг, для забезпечення маршрутизації їх інформаційних потоків шляхом моніторингу, кращих практик та оновлення інформації про маршрутизацію в Регістрі Інтренет маршрутизації IRR (Internet Routing Registry), в ідеалі включаючи дійсну Авторизацію походження маршруту ROA (Route Origin Authorisation).

Висновки та перспективи подальших досліджень. В роботі показано, що при використанні в мережі протоколу BGP забезпечення безпеки передачі інформаційних потоків виходить на новий рівень важливості та цінності. В результаті проведеного аналізу були виділені 3 групи вразливостей для безпеки, які пов'язані з повідомленнями, безпекою на транспортному рівні та з інфраструктурою. Показано, що на сьогоднішній день, незважаючи на це, немає загальних вимог щодо безпеки, головних цілей покращення чи критеріїв кінцевого рішення.

Всі рішення, що були створенні на момент написання статті і розглянуті в даній роботі, дуже різноманітні, деякі наслідують попередні пропозиції, деякі зовсім ні на що не схожі. Показано, що через відсутність чітко сформульованих вимог багато часу йде на вивчення запропонованих рішень, порівняння з раніше відомими та вирішення щодо їх практичного використання. Крім того описані етапи та проблеми тестування нових рішень від початкової теоретичної оцінки до можливості вводу в експлуатацію або ж відмови від подальшої розробки. Наведено обґрунтування великих часових витрат саме на процес тестування. Також представлені деякі з причин випадків відмови від представлення користувачам рішень, що успішно пройшли тестування. Згадується й економічний аспект, який відіграє

не останню роль у впроваджені нових рішень в загальну експлуатацію і лягає повністю на плечі провайдерів та операторів мережі, які, в свою чергу виражають супротив такому положенню справ.

Все це стало причинами того, що проблема вразливості мережі Інтернет не просто є актуальною, а й наближається до статусу такої, «що не вирішується» в найкоротший час для багатьох користувачів.

В роботі доведено, що на даний час найкращим способом забезпечення маршрутизації BGP є використання індивідуальної безпеки через застосування таких практик безпеки, як розробка фільтрів маршрутів, використання та оновлення інформації про маршрутизацію, наявну в IRR, та моніторинг. Проте, можливо, зараз ще не досягнутий той рівень розвитку технології BGP, при якому можливе використання безпечної маршрутизації за замовчуванням. Це може бути додатковою послугою, яка пропонується провайдерами або зовнішніми компаніями. Показано, що вже сьогодні є компанії, які надають послуги з моніторингу безпеки BGP на основі власної розгорнутої інфраструктури. Компанії, що надають контент-мережу (CDN), можуть також надавати послуги безпеки BGP своїм клієнтам на основі їх мережевої інфраструктури. Доведено, що користувачам, для яких безпека передачі інформаційних потоків в мережі Інтернет є критичним питанням вже зараз і які не можуть чекати розробки та впровадження розширення, яке б вирішило усі проблеми безпеки функціонування BGP, такий підхід був би необхідним та оптимальним вже зараз.

Список бібліографічних джерел

1. Apostolaki, M., Zohar, A. & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 375–392.
2. Rekhter, Y., Sangli, S. R. & Tappan, S. (2006). RFC 4360: BGP Extended Communities Attribute.
3. Lepinski, M. & Sriram, K. (2017). RFC 8205: BGPsec Protocol Specification.
4. White, R. (2003). Securing BGP Through Secure Origin BGP. *The Internet Protocol Journal, 2003, vol. 6, № 3*.
5. McPherson, D. & Scudder, J. G. (2007). RFC 5065: Autonomous System Confederations for BGP.
6. Chandra, R., Chen, E. & Bates, T. (2000). RFC 2796: BGP Route Reflection – An Alternative to Full Mesh IBGP.
7. Snijders, J., Bagdonas, I., Patel, K., Heitz, J. & Hilliard, N. (2017). RFC 8092: BGP Large Communities Attribute.
8. Chen, E. (2000) RFC 2918: Route Refresh Capability for BGP-4.
9. Chandra, R. & Scudder, J. G. (2000). RFC 2842: Capabilities Advertisement with BGP-4.
10. Fernando, R., Sangli, S. R., Rekhter, Y., Chen, E. & Scudder, J. G. (2007). RFC 4724: Graceful Restart Mechanism for BGP.
11. Villamizar, C., Govindan, R. & Chandra, R. (1998). RFC 2439: BGP Route Flap Damping.
12. Heffernan, A. (1998). RFC 2385: Protection of BGP Sessions via the TCP MD5 Signature Option.
13. Touch, J., Mankin, A. & Bonica, R. P. (2010). RFC 5925: The TCP Authentication Option.
14. Savola, P., Gill, V., Pignataro, C., Meyer, D. & Heasley, J. (2007). RFC 5082: The Generalized TTL Security Mechanism (GTSM).
15. Subramanian, L., Roth, V., Stoica, I., Shenker, S. & Katz, R. H. (2004). Listen and Whisper: Security Mechanisms for BGP. *1st Symposium Networked System Design and Implementation*, pp. 14-16.

References

1. Apostolaki, M., Zohar, A. & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 375–392.
2. Rekhter, Y., Sangli, S. R. & Tappan, S. (2006). RFC 4360: BGP Extended Communities Attribute.
3. Lepinski, M. & Sriram, K. (2017). RFC 8205: BGPsec Protocol Specification.
4. White, R. (2003). Securing BGP Through Secure Origin BGP. *The Internet Protocol Journal, 2003, vol. 6, № 3*.
5. McPherson, D. & Scudder, J. G. (2007). RFC 5065: Autonomous System Confederations for BGP.
6. Chandra, R., Chen, E. & Bates, T. (2000). RFC 2796: BGP Route Reflection – An Alternative to Full Mesh IBGP.
7. Snijders, J., Bagdonas, I., Patel, K., Heitz, J. & Hilliard, N. (2017). RFC 8092: BGP Large Communities Attribute.
8. Chen, E. (2000) RFC 2918: Route Refresh Capability for BGP-4.
9. Chandra, R. & Scudder, J. G. (2000). RFC 2842: Capabilities Advertisement with BGP-4.
10. Fernando, R., Sangli, S. R., Rekhter, Y., Chen, E. & Scudder, J. G. (2007). RFC 4724: Graceful Restart Mechanism for BGP.
11. Villamizar, C., Govindan, R. & Chandra, R. (1998). RFC 2439: BGP Route Flap Damping.
12. Heffernan, A. (1998). RFC 2385: Protection of BGP Sessions via the TCP MD5 Signature Option.
13. Touch, J., Mankin, A. & Bonica, R. P. (2010). RFC 5925: The TCP Authentication Option.
14. Savola, P., Gill, V., Pignataro, C., Meyer, D. & Heasley, J. (2007). RFC 5082: The Generalized TTL Security Mechanism (GTSM).
15. Subramanian, L., Roth, V., Stoica, I., Shenker, S. & Katz, R. H. (2004). Listen and Whisper: Security Mechanisms for BGP. *1st Symposium Networked System Design and Implementation*, pp. 14-16.

Рецензію надав к.т.н., доцент кафедри інформаційних технологій Київського національного університету будівництва і архітектури Щербина Олександр Андрійович