УДК 004.738.5

Н.Н. МИНАКОВА, А.В. МАНСУРОВ

РЕШЕНИЕ ДЛЯ ОБНАРУЖЕНИЯ И БЛОКИРОВКИ РАСПРОСТРАНЕНИЯ АНОМАЛЬНОЙ МАРШРУТНОЙ ИНФОРМАЦИИ ПРОТОКОЛА BGP-4

В данной статье обсуждается вариант решения для обнаружения и предотвращения распространения аномальной маршрутной информации, распространяемой по протоколу BGP-4. Предлагаемое решение не требует модификации стандартного программного обеспечения маршрутизаторов оператора связи, что дает возможность для его плавной интеграции без перерывов в обеспечении услуг связи. Анализ и проверка правильности распространяемых маршрутов базируется на данных из баз данных регистратур маршрутной информации организаций – координаторов межсетевого взаимодействия в сети Интернет. Алгоритм приведенного решения строит проверку пути распространения каждого маршрута в соответствии с декларируемой политикой связности всех операторов связи по цепочке и исключает попадание некорректных маршрутов, появившихся вследствие «утечек», «угонов» или ошибочных конфигураций маршрутизаторов транзитных операторов на любом участке, в таблицы маршрутизации контролируемого данным решением оператора связи. Решение является модульным, и его функциональность может быть расширена и адаптирована как расширением возможностей алгоритма анализа маршрутной информации, так и увеличением числа агентов, выполняющих непосредственное удаленное взаимодействие с пограничными маршрутизаторами контролируемого оператора связи по блокировке поступающих аномальных маршрутов в соответствии со спецификой командного интерфейса управления маршрутизаторов.

Ключевые слова: *Border Gateway Protocol (BGP-4), сетевая безопасность, безопасность BGP, маршрутизация, BGP связность, оператор связи.*

Введение

Современная всемирная сеть Интернет является сложной структурой, основанной на взаимоувязанной работе множества независимых операторов связи друг с другом, что в терминах технического межсетевого взаимодействия и обмена транспортируемыми данными описывается как связность автономных систем (АС) между собой с использованием протокола обмена маршрутной информацией BGP-4 (Border Gateway Protocol ver. 4) [1]. Под «автономной системой» (АС) в таких случаях традиционно понимается условная «зона ответственности» оператора связи с принадлежащими ему маршрутизаторами, находящимися под единым административным управлением и использующими единый согласованный план внутренней маршрутизации, а также согласованную картину адресатов, доступных через данную АС. Протокол BGP-4 уже более 20 лет формирует надежную основу межоператорского взаимодействия благодаря своей надежности, эффективности и гибкости, принимая во внимание сетевые конфигурации любой сложности как внутри АС, так и образуемые взаимосвязью множества разных АС.

Тем не менее, протокол BGP-4 не лишен проблем, связанных с безопасностью его работы в части механизма принятия решения об оптимальности выбранного маршрутного пути [2-4]. Среди проблем отмечается сильная ориентированность на атрибут AS_PATH маршрута-префикса в процессе принятия решения, а также отсутствие возможности встроенной верификации «легитимности» распространяемого по цепочке транзита маршрута-префикса. Это приводит к появлению «утечек» и «угонов» маршрутов (ситуаций, при которых маршруты-префиксы той же самой длины или более мелкие/специфичные анонсируются от имени другой АС – случайно или преднамеренно).

Среди ключевых моментов в спектре предлагаемых решений [5-7] обозначенных проблем можно выделить либо необходимость анализа и выявления аномалий распространяемой маршрутной информации, либо внедрение в распространяемую маршрутную информацию специальных криптографических подписей-хешей для однозначного установления подлинности маршрута-префикса и легитимности его пути распространения. Однако, переход к использованию цифровых подписей (протокол BGPSec) [6] влечет за собой отказ от действующего стандарта протокола BGP-4 и переход к поддержке нового протокола маршрутизации всеми участниками сетевого взаимодействия, что в условиях декларированной независимости функционирования каждой АС является маловероятным. В этом случае, методика осуществления анализа маршрута-префикса и его атрибутов является более «мягкой» для применения, поскольку может выполняться независимо от работы самого алгоритма протокола BGP-4. Результаты анализа могут быть использованы для корректировки работы протокола BGP-4 его штатными средствами, реализованными на мар-

шрутизаторах (такими как community, local preference, механизмы фильтрации принимаемой и анонсируемой маршрутной информации) [1].

Ранее в работе [8] авторами было предложено решение, развивающее метод анализа и выявления аномалий в маршрутной информации с возможностью корректировки работы маршрутизаторов контролируемой АС. Несмотря на хорошие полученные результаты, предложенное решение осуществляет анализ пути распространения маршрута-префикса на основе информации AS_PATH с небольшой глубиной пути, что соответствует непосредственным соседям, связанным с контролируемой АС (аплинки, клиентские и пиринговые взаимодействия). В данной работе рассматривается усовершенствованный и оптимизированный алгоритм обработки и анализа маршрутной информации с более детальным и полным анализом пути распространения маршрута-префикса, что позволяет сформировать более комплексный алгоритм выявления аномалий, увеличить глубину контроля и пресечь распространение некорректной маршрутной информации, которая может привести к дальнейшей дестабилизации межсетевого взаимодействия.

Программная реализация предлагаемого решения

Сформированное решение, аналогично решению [8], подключается к сети контролируемой АС (к одному из маршрутизаторов) по протоколу BGP-4 в качестве внутреннего участника (используется номер контролируемой АС при условии, что в контролируемой АС не применяются конфедерации) и получает все поступающие в контролируемую АС обновления маршрутной информации. Структурная схема решения (рис. 1) содержит основные алгоритмические блоки, которые отвечают за прием и обработку обновлений по протоколу BGP-4, выполнение анализа и формирование реакции на обнаруженную аномалию в маршруте. Для обеспечения гибкости работы алгоритмические блоки рассинхронизированы через связующие очереди обработки и могут рассматриваться как сущности с достаточной долей самостоятельности в своей работе.

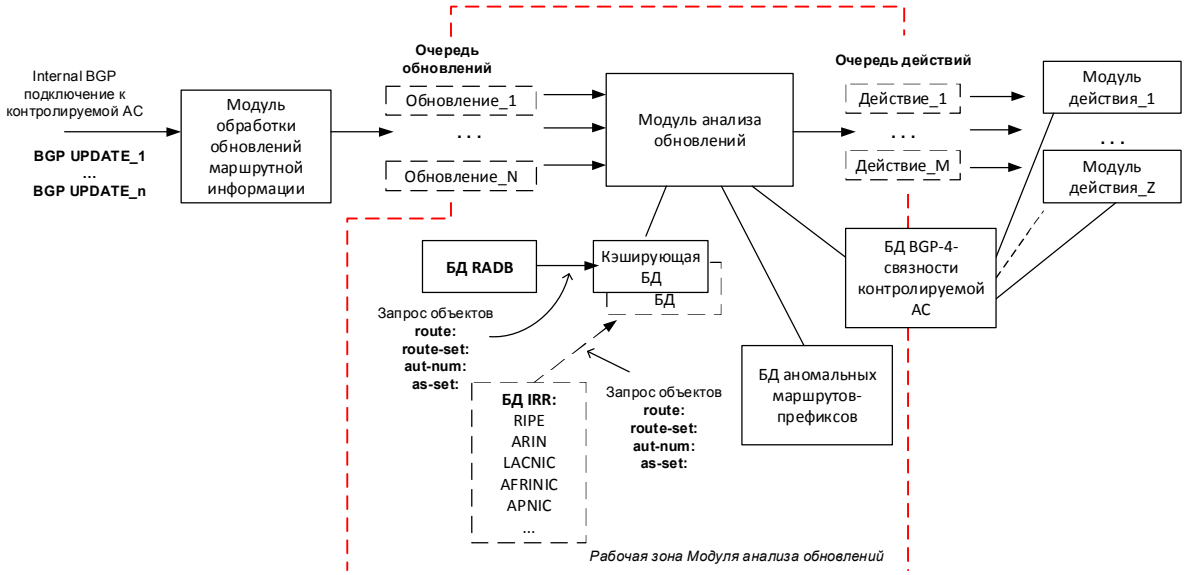

Рис. 1. Структурная схема решения для анализа и выявления аномалий в маршрутной информации с последующей генерацией корректирующих действий для контролируемой АС на основе схемы в [8]

Обработка каждого поступившего обновления маршрутной информации осуществляется в модуле «Модуль обработки обновлений маршрутной информации». Задача модуля – сформировать на основании приходящих UPDATE-сообщений (type = 2) векторы, содержащие следующую информацию:

- путь в виде цепочки АС (AS_PATH) длиной P элементов с реверсированием последовательности и исключением многократно повторяющихся номеров одной и той же АС в общей цепочке (если кто-то использует механизм искусственного удлинения пути AS-PATH Prepend);
- IP-адрес «следующего» маршрутизатора BGP-соседа (соседней АС) (NEXT_HOP);
- прикрепленный к маршрутной информации набор BGP communities [9];
- анонсируемые маршруты (Network Layer Reachability Information – NLRI).

Сформированные векторы являются входными для следующего модуля и формируют «Очередь обновлений».

«Модуль анализа обновлений» осуществляет работу со сформированными входными векторами из «Очереди обновлений». Для анализа и проверки маршрутной информации используются глобальные базы данных (БД), описывающих политики и маршрутизации и связности для составляющих глобальную сеть Интернет АС. Это - RADb (Routing Assets Database) [10] и базы данных, входящие в список регистратур маршрутной информации сети Интернет – The Internet Routing Registry (IRR) [11], поддерживающие RPSL (RFC2622) [12] или свой собственный язык описания объектов маршрутной информации. Структурная схема работы предлагаемого алгоритма при работе со сформированной «Очередью обновлений» приведена на рисунке 2.

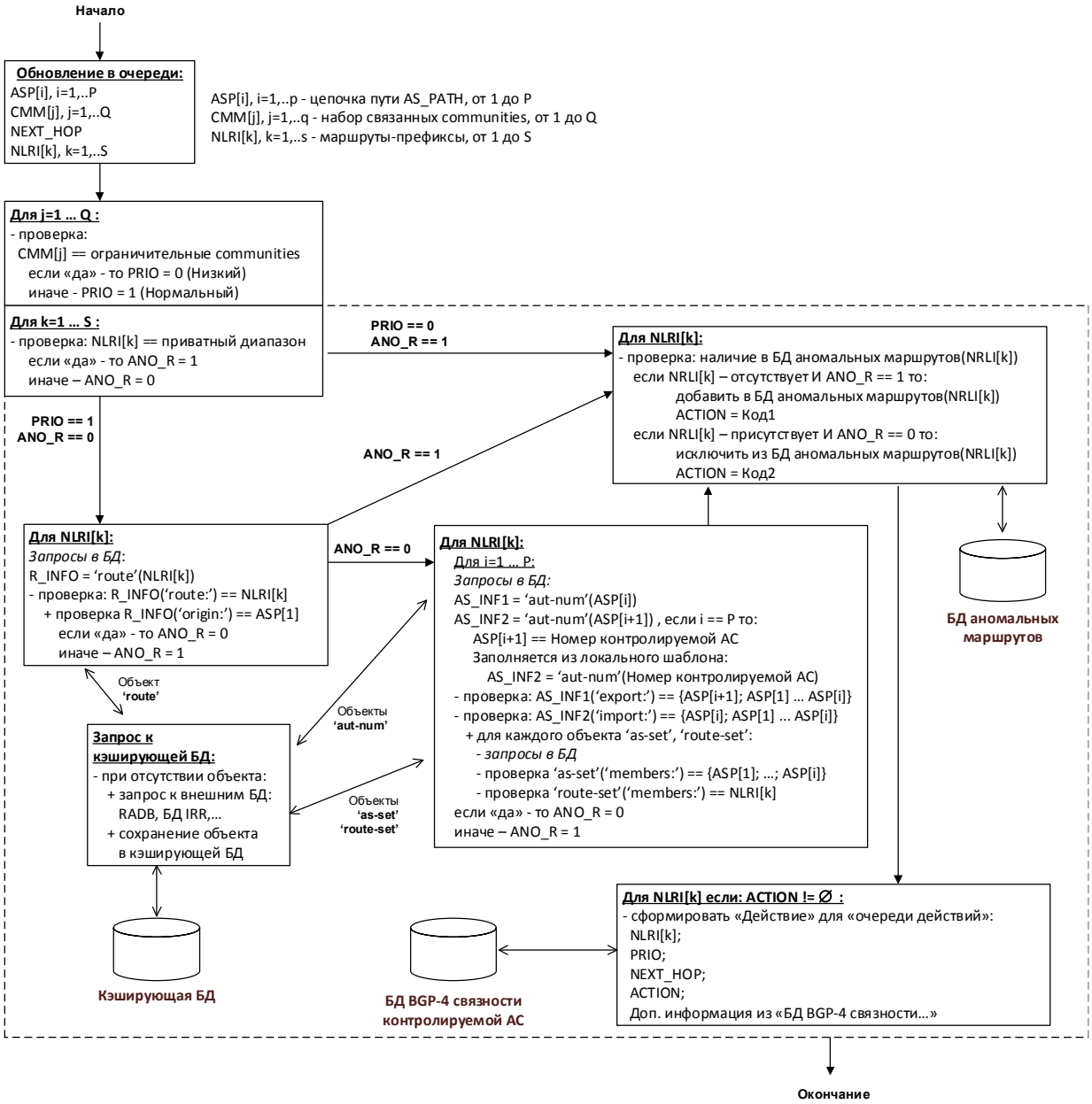

Рис. 2. Структурная схема предлагаемого алгоритма анализа маршрутной информации при работе со сформированной «Очередью обновлений»

Процесс работы оптимизированного алгоритма анализа строится следующим образом:

1) анализ содержащегося во входном векторе BGP communities (CMM[j]) на наличие ограничительных community - no-advertise или иных ограничительных community политики управления маршрутной информации (например, понижение local preference), принятой в контролируемой АС. При совпадении – устанавливается внутренняя метка приоритетности (PRIO) для обрабатываемого входного вектора в значение «низкий»;

2) разбиение пути в виде цепочки АС (AS_PATH) на набор отдельных элементов ASP[i] с сохранением порядка;
3) проверка маршрутов-префиксов NLRI[k], содержащихся в обрабатываемом входном векторе, на совпадение с диапазонами приватных сетей, которые не должны анонсироваться. При совпадении – проверка заканчивается, маршрут-префикс помечается (метка ANO_R) как не прошедший проверку и «*аномальный*» (ANO_R = 1). Проверка также заканчивается при значении метки приоритетности, равной «низкому». В этом случае детальный анализ и проверка маршрутной информации на последующих шагах 4) и 5) будут излишними, поскольку с большой долей вероятности маршрутная информация в данном обновлении не будет являться активной в таблицах маршрутизации BGP-устройств контролируемой АС или не покинет пределы контролируемой АС;
4) для каждого непомеченного маршрута-префикса NLRI[k] (после шага 3)) запрашивается объект '**route**' из локальной кеширующей БД, а при отсутствии – непосредственно из БД RADb или (при отсутствии в БД RADb) в других БД IRR для сравнения содержащихся в запрошенном объекте полей 'route:' и 'origin:' со значениями обрабатываемого маршрута-префикса и самого первого элемента из цепочки пути АС (ASP[1]), который является номером начальной АС – источника данного маршрута-префикса. При отличиях – проверка заканчивается, маршрут-префикс помечается как не прошедший проверку и «*аномальный*» (ANO_R = 1). Запрошенные объекты '**route**' из внешних БД сохраняются в локальной кеширующей БД;
5) для каждого непомеченного маршрута-префикса NLRI[k] (после шага 4)) запрашивается объект '**aut-num**' для каждого элемента, начиная с самого первого ASP[1], из цепочки пути АС (AS_PATH) по порядку следования до окончания набора элементов ASP[P] в цепочке пути АС. Запрос выполняется к локальной кеширующей БД, а при отсутствии в ней объекта – непосредственно к БД RADb или (при отсутствии в БД RADb) к другим БД IRR. Сравниваются и анализируются:
   - поле 'export:' у объекта, соответствующего текущему элементу ASP[i] в цепочке пути АС, для установления вхождения номера АС, соответствующего следующему элементу ASP[i+1] в цепочке пути АС (относительно текущего), и списка анонсируемых номеров АС для установления совпадения с номером текущей анализируемой АС;
   - поле 'import:' у объекта, соответствующего следующему элементу ASP[i+1] в цепочке пути АС (относительно текущего), для установления вхождения номера АС, соответствующего текущему элементу ASP[i] в цепочке пути АС, и списка принимаемых номеров АС для установления совпадения с номером текущей анализируемой АС;
   - при наличии в списке анонсируемых или принимаемых номеров АС указаний на групповые объекты – запрашиваются способом, аналогичным приведенному в данном шаге ранее, указанные групповые объекты '**as-set**' и '**route-set**' для последующего анализа полей 'members:' и установления вхождения номера текущей анализируемой АС или текущего анализируемого маршрута-префикса;

   При установлении всех требуемых вхождений маршрут-префикс помечается как прошедший проверку, в противном случае - как не прошедший проверку и «аномальный» (ANO_R = 1);

   Все запрошенные объекты из внешних БД сохраняются в локальной кеширующей БД;

   При достижении последнего элемента ASP[P] в цепочке пути АС в качестве следующего элемента назначается номер контролируемой АС, для которой используются хранящиеся локально актуальные объекты '**aut-num**', '**as-set**' и '**route-set**' (при наличии). Данный этап завершает анализ и проверку исследуемого маршрута-префикса, производится переход к следующему маршруту-префиксу (при наличии);
6) для всех маршрутов-префиксов выполняется проверка в локальной «БД Аномальных маршрутов»:
   - маршруты-префиксы, помеченные по итогам анализа как «аномальные» и отсутствующие в указанной БД, добавляются в нее с установлением дополнительной внутренней метки «*действие*» (ACTION) со значением определенного кода. Если «аномальные» маршруты уже присутствует в указанной БД, то дополнительных действий не производится;

- маршруты-префиксы, не помеченные по итогам анализа как «аномальные», но присутствующие в указанной БД, исключаются из нее с установлением дополнительной внутренней метки «*действие*» со значением определенного кода;

7) для всех маршрутов-префиксов с внутренней меткой «*действие*» (ACTION) формируются векторы, которые являются входными для следующего модуля и образуют «Очередь действий». В сформированные векторы добавляется дополнительная информация о точке локализации каждого маршрута-префикса, которая запрашивается из БД «BGP-4 связность контролируемой АС». В этой БД хранится информация об адресах пограничных маршрутизаторов, BGP-соседях каждого пограничного маршрутизатора, типе оборудования (производителе) и т.п.

Локальная кеширующая БД используется для хранения ранее запрошенных объектов из внешних БД в течение 24 часов (время хранения может быть изменено по требованию) и необходима для снижения нагрузки на БД регистратур маршрутной информации (RADb и IRR).

«Модули действий» выполняют работу с «Очередью действий» и активизируются в соответствии с установленными кодами (например, закодированными битами-триггерами в метке «*действие*»). Само действие может включать в себя уведомление системных администраторов контролируемой АС, внесение или исключение аномального маршрута-префикса в/из список/ка блокировки в конфигурации соответствующего маршрутизатора контролируемой АС и пр.

Программное исполнение решения выполнено на языке программирования Python. Взаимодействие по протоколу BGP-4 выполняется с использованием BGP-агента YABGP [13]. В качестве локальных БД используется документоориентированная БД mongoDB [14], которая позволяет эффективно хранить объекты БД RADb и IRR, осуществлять поиск и выборку требуемой информации по сохраненным объектам, а также хранить информацию о топологии и связности BGP-маршрутизаторов контролируемой АС.

Заключение

В работе было предложено решение для контроля и выявления аномалий в маршрутной информации, распространяемой по протоколу BGP-4. Предложенное решение развитием предыдущих наработок коллектива авторов и включает в себя оптимизацию работы основного алгоритма выполнения анализа и обнаружения аномалий с прослеживанием всего пути распространения маршрутов-префиксов до ее поступления в зону ответственности контролируемой АС. Решение не требует модификации программного обеспечения используемых в контролируемой АС BGP-маршрутизаторов и легко интегрируется в сетевую конфигурацию контролируемой АС. Решение подходит для транзитного оператора связи регионального или национального масштаба с наличием развитой связности с АС других операторов.

Дальнейшее развитие предложенного решения предполагает расширение поддерживаемого синтаксиса RPSL, адаптацию для работы в более сложных сетевых конфигурациях (конфедерации, MED, поддержка маршрутной информации IPv6), а также получение и обработку данных о маршрутных аномалиях из внешних источников, ведущих независимый мониторинг BGP-связности АС в сети Интернет.

Авторы благодарят Щетинина Д.С. за всестороннюю техническую поддержку работы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Rekhter Y., Li T., Hares S. RFC 4271 - A Border Gateway Protocol 4 (BGP-4). URL: https://tools.ietf.org/html/rfc4271
2. Patel K., Meyer D. RFC 4274 - BGP-4 Protocol Analysis. URL: https://tools.ietf.org/html/rfc4274
3. Smith J., Birkeland K., Schuchard M. An Internet-Scale Feasibility Study of BGP Poisoning as a Security Primitive. 2018. DOI: arXiv:1811.03716v5 [cs.CR]
4. Butler K., Farley T., McDaniel P., Rexford J. A Survey of BGP Security Issues and Solutions // Proceedings of the IEEE. 2009. Vol. 98. Issue 1. P. 100-122. DOI: 10.1109/JPROC.2009.2034031
5. Hiran R., Carlsson N., Shahmehri N. Does scale, size, and locality matter? Evaluation of collaborative BGP security mechanisms // Proc. Of the IFIP Networking, 2016. P. 261-269. DOI: 10.1109/IFIPNetworking.2016.7497237
6. Lepinski M., Sriram K. RFC8205 - BGPsec Protocol Specification. URL: https://tools.ietf.org/html/rfc8205
7. Li Q., Liu J., Hu Y., Xu M., Wu J. BGP with BGPsec: Attacks and Countermeasures // IEEE Network. 2018. P. 1-7. DOI: 10.1109/MNET.2018.1800171
8. Мансуров А.В., Щетинин Д.С. С. Решение для автоматизированного выявления и предупреждения аномалий маршрутной информации, распространяемой по протоколу BGP-4 // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. 2019. № 08. С. 78-84

9. Chandra R., Traina P. RFC 1997 - BGP Communities Attribute. URL: https://tools.ietf.org/html/rfc1997
10. The Internet Routing Registry - RADb. URL: https://www.radb.net/
11. List of Routing Registries – The Internet Routing Registry (IRR). URL: http://www.irr.net/docs/list.html
12. Routing Policy Specification Language (RPSL). URL: https://tools.ietf.org/html/rfc2622
13. YABGP Project. URL: https://yabgp.readthedocs.io/en/latest/
14. mongoDB. URL: https://www.mongodb.com/

Минакова Наталья Николаевна
Д-р физ.-мат. наук, профессор,
Профессор кафедры информационной безопасности
Алтайский государственный университет
656049, Россия, г. Барнаул, Ленина пр-т, д. 61,
Тел.: +7-905-985-71-05
Эл. почта: minakova@phys.asu.ru

Мансуров Александр Валерьевич
Канд. техн. наук, доцент кафедры
информационной безопасности
Алтайский государственный университет
656049, Россия, г. Барнаул, Ленина пр-т, д. 61,
Тел.: +7-903-910-81-73
Эл. почта: mansurov.alex@gmail.com

N.N. MINAKOVA, A.V. MANSUROV

AN OPEN-SOURCE SOLUTION FOR DETECTION AND BLOCKING OF ANOMALOUS BGP-4 ROUTES

This paper discusses an open-source solution for detection and blocking of anomalous BGP-4 routes. The proposed solution does not require any changes or upgrades of the existing software or firmware of deployed network routers, thus, it can be easily adopted by any regional or national telecom operators for protection against unexpected routing incidents. Propagated BGP-4 route updates are analyzed using the up-to-date routing databases maintained by Internet registries. The analysis algorithm of the proposed solution checks the propagated path of each route according to the declared connectivity policies of each telecom operator along the path to identify and block the hijacked or leaked routes caused by actions with malicious intents or misconfiguration of transit routers somewhere outside the scope of the "protected" telecom operator. The solution has modular design and allows flexible enhancements of its functionality of the analysis module and its algorithm, or the action modules that provide remote control and automated configuration of network routers according to the vendor specifics.

Keywords: *Border Gateway Protocol (BGP-4), BGP security, network security, routing, BGP connectivity, telecom operator.*

REFERENCES

1. Rekhter Y., Li T., Hares S. RFC 4271 - A Border Gateway Protocol 4 (BGP-4). URL: https://tools.ietf.org/html/rfc4271
2. Patel K., Meyer D. RFC 4274 - BGP-4 Protocol Analysis. URL: https://tools.ietf.org/html/rfc4274
3. Smith J., Birkeland K., Schuchard M. An Internet-Scale Feasibility Study of BGP Poisoning as a Security Primitive. 2018. DOI: arXiv:1811.03716v5 [cs.CR]
4. Butler K., Farley T., McDaniel P., Rexford J. A Survey of BGP Security Issues and Solutions. *Proceedings of the IEEE*. 2009. Vol. 98. Issue 1. P. 100-122. DOI: 10.1109/JPROC.2009.2034031
5. Hiran R., Carlsson N., Shahmehri N. Does scale, size, and locality matter? Evaluation of collaborative BGP security mechanisms. *Proc. IFIP Networking*. 2016. P. 261-269. DOI: 10.1109/IFIPNetworking.2016.7497237
6. Lepinski M., Sriram K. RFC8205 - BGPsec Protocol Specification. URL: https://tools.ietf.org/html/rfc8205
7. Li Q., Liu J., Hu Y., Xu M., Wu J. BGP with BGPsec: Attacks and Countermeasures. *IEEE Network*. 2018. P. 1-7. DOI: 10.1109/MNET.2018.1800171
8. Mansurov A.V., Schetinin D.S. Automatic detection and distribution prevention of incorrect BGP-4 routing information. *Modern Science: actual problems of theory & practice. Series Natural and Technical Science*. 2019. No. 9. P. 78-84 (in Russian).
9. Chandra R., Traina P. RFC 1997 - BGP Communities Attribute. URL: https://tools.ietf.org/html/rfc1997
10. The Internet Routing Registry - RADb. URL: https://www.radb.net/
11. List of Routing Registries – The Internet Routing Registry (IRR). URL: http://www.irr.net/docs/list.html
12. Routing Policy Specification Language (RPSL). URL: https://tools.ietf.org/html/rfc2622
13. YABGP Project. URL: https://yabgp.readthedocs.io/en/latest/
14. mongoDB. URL: https://www.mongodb.com/

Natalya N. Minakova
Doctor of Physics and Mathematics, Professor,
Department of Information Security
Altai State University,
61, Lenina ave., Barnaul, Russia, 656049
Phone: +7-905-985-71-05,
E-mail: minakova@phys.asu.ru

Alexander V. Mansurov
PhD of Technical Sciences, Associate Professor,
Department of Information Security
Altai State University,
61, Lenina ave., Barnaul, Russia, 656049
Phone: +7-903-910-81-73,
E-mail: mansurov.alex@gmail.com