Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 21 – 24 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

BGP (BORDER GATEWAY PROTOCOL) მარშრუტიზაციის პროტოკოლი და თანამედროვე საფრთხეები

არჩილი შენგელია[1]
[1]სოხუმის სახელმწიფო უნივერსიტეტი, თბილისი, საქართველო

ABSTRACT: It is difficult to imagine today's modern world without the Internet. The Internet has become very popular in the last 30 years and has changed many aspects of our daily existence. Our world has become highly dependent on Internet technologies and systems, and many essential services that billions of people use every day would simply not be available without Internet communications and networks. On the other hand, the almost continuous connection of billions of devices in Internet communications has led to an unhealthy interest of various types of cybercriminals in global computer networks, and for many organizations, the threat of hijacking, theft or destruction of their data and various values has potentially increased.

საკვანძო სიტყვები: *გლობალური მარშრუტიზაცია, მარშრუტიზაციის პროტოკოლების საფრთხეები და სისუსტეები*

1. შესავალი

BGP პროტოკოლი არის მარშრუტიზაციის ვექტორული პროტოკოლი, რომელიც ძირითადად გამოიყენება საშუალო და დიდი ზომის ინტერნეტ პროვაიდერების მიერ გლობალურ ქსელში მილიონობით მარშრუტიზაციის ჩანაწერის ურთიერთგაზიარებისათვის. პროტოკოლი იყენებს ეგრეთწოდებულ ავტონომიურ სისტემებს (AS – Autonomous Systems), რომელთა შიგნითაც ხდება განთავსება ხშირად ცალკეული ქვეყნისა და რეგიონის მრავალმილიონიანი ტრაფიკის დამმუშავებელი ე.წ. Border ანუ მოსაზღვრე მარშრუტიზატორებისა. თვით ავტონომიური სისტემა წარმოადგენს დამოუკიდებლად მოქმედ ქსელს,რომელიც იყენებს BGP მარშრუტიზაციის პროტოკოლს და მასში გამოცხადებული ყველა მარშრუტი ექვემდებარება საერთო წესებს. ყოველ ავტონომიურ სისტემას გააჩნია ავტონომიური სისტემის ნომერი ASN – Autonomous System Number, რომელიც ახდენს მასში წარმოდგენილი ქსელების უნიკალურობის იდენტიფიცირებას.

2. BGP პროტოკოლი და მისი სტანდარტები

საერთაშორისო სტანდარტიზაციის ორგანიზაციამ IANA – Internet Assign Numbers Authority, რომელიც მთელს მსოფლიოში ახდენს გლობალურ კოორდინირებას DNS Root, IP მისამართების დიაპაზონებისა და სხვადასხვა ინტერნეტ პროტოკოლების შემუშავება/იმპელენტაციაზე, შეიმუშავა წესების ნაკრები, რომელიც სავალდებულოა ყველა ქსელური თუ კომპიუტერული სისტემების მწარმოებელი კომპანიებისათვის [1-2]. IANA-მ მსოფლიოს 5 ძირითად რეგიონში (ARIN - კანადა, აშშ და რამოდენიმე კარიბის ზღვის კუნძული, LACNIC - ლათინური ამერიკა, RIPE NCC - ევროპა,შუა აზია და ცენტრალური აზიის ქვეყნები, APNIC - აზია, წყნარი ოკეანის ქვეყნები და AFRINIC - აფრიკის კონტინენტის ქვეყნები) ოპერირების მქონე ინტერნეტ სერვის პროვაიდერებს შესასრულებლად სავალდებულოდ დაუწესა მრავალფეროვანი ქსელური პროტოკოლებისა და მათი ნაკრებების დანერგვა/გამოყენების პარამეტრები. მათ შორის

IANA-მ 1994 წელს გამოაქვენა RFC 1654 სტანდარტის სახით დინამური მარშრუტიზაციის ვექტორული პროტოკოლი სახელწოდებით BGP – Border Gateway Protocol.
საერთასორისო ორგანიაზია IANA გასცემს ASN-ს ე.წ. RIR – Regional Internet Registries-ზე, რომელნიც თავის მხრივ სისტემის შიგნით თავიანთ ოპერირების ზონებში არეგისტრირებენ შიდა მოხმარების ავტონომიურ სისტემებს და ანიჭებენ მათ სერვისების გამომყენებელ ორგანიზაციებს. BGP პროტოკოლის ძირითადი დანიშნულება გახლავთ სწორედ AS-ს შორის კავშირის ხელმისაწვდომობაზე კონტროლი და მარშრუტების ურთიერთგაცვლა. მარშრუტები, რომელიც იცვლება სხვადასხვა ქვეყნის AS-შ შორის მუშავდება eBGP – External Border Gateway Protocol მიერ,ხოლო მარშრუტები ქვეყნის შიგნით განლაგებულ AS-ს შორის მუშავდება iBGP – Internal Border Gateway Protocol-ის მიერ [3-5].

3. BGP მოწყვლადობების ტაქსონომია

BGP პროტოკოლის სტრუქტურაში გამოვლინდა ქვემოთ ჩამოთვლილი სისუსტეები:

- **მარშრუტის გადაჭერა (Route Hijacking):** კრიტიკული სისუსტე,რომლის მეშვეობითაც შემტევ მხარეს შეუძლია გამოაცხადოს ყალბი მარშრუტები.შედეგად შესაძლოა განხორციელდეს რესურსებზე არაავტორიზირებული წვდომა,მათი მოდიფიკაცია ან სერვისების გაუმართაობა
- **მარშრუტების გაჟონვა (Route Leaks):** მარშრუტიზაციის ინფორმაციის შემთხვევითი ან განზრახ გამჟღავნება მისი დანიშნულების ფარგლებს გარეთ, რაც იწვევს მონაცემთა ნაკადში არასასურველ ცვლილებებს.
- **BGP პრეფიქსების დეაგრეგაცია (BGP Prefix Deaggregation):** ზედმეტად სპეციფიკური პრეფიქსების გავრცელება ხელს უწყობს მარშრუტიზაციის ცხრილის ინფლაციას, რაც ქსელებს დაუცველს ხდის DDos შეტევების მიმართ.
- **BGP სესიის გადაჭერა (BGP Session Hijacking):** დამნაშავეები გადაჭერილი სესიების მეშვეობით წარმოაჩენენ საკუთარ მოწოდებულ ინფორმაციას, როგორც კანონიერი მარშრუტიზატორებიდან მოწოდებულს, რითაც შესაძლებელი ხდება ქსელური ტრაფიკით მანიპულირება.
- **BGP სესიის განულება (BGP Session Reset):** სეანსების განულება მათი რეალიზებისას დამნაშავეების მიერ სპეციალურად დაშვებული შეცდომების გამო იწვევს ქსელის არასტაბილურ მუშაობას.
- **BGP პრეფიქსის მანიპულირება (BGP Prefix Manipulation):** BGP ატრიბუტებით მანიპულირებით, დამნაშავეებს შეუძლიათ ზემოქმედება მარშრუტების არჩევასა და ტრაფიკის მთლიანად გადამისამართებაზე.

4. BGP მოწყვლადობების პოტენციური შედეგები

- **მონაცემების გადაჭერა (Data Interception):** შემტევებს შეეძლებათ გადაამისამართონ ტრაფიკი საკუთარი ქსელების მიმართულებაზე, რაც აუცილებლად შექმნის საფრთხეს კონფიდენციალური ინფორმაციის გადაჭერისა.
- **მონაცემების მოდიფიკაცია (Data Modification):** შემტევებს შეეძლებათ გადასაცემი მონაცემების შიგთავსის შეცვლა, რაც აუცილებლად გამოიწვევს მონაცემების გაჟონვასა და მათზე არასანქცირებულ წვდომას.
- **მომსახურეობის დარღვევა (Service Disruption):** მარშრუტების გადაჭერა ან გაჟონვა აუცილებლად გამოიწვევს ქსელების მუშაობის ხარისხის დეგრადაციას.

- **DDos ამპლიფიკაცია (DDos Amplification):** BGP პრეფიქსების დეაგრეგაცია შესაძლოა გამოყენებულ იქნეს დამნაშავეების მიერ ქსელებზე DDos შეტევისას უფრო მეტი ზიანის მისაყენებლად.
- **სანდოობის დარღვევა (Trust Erosion):** უსაფრთხოების ხშირი დარღვევები მნიშვნელოვნად აქვეითებს ორგანიზაციების ნდობას ინტერნეტ მარშრუტიციის ინფრასტრუქტურის მიმართ,რაც პოტენციურად გამოიწვევს საერთო შემოსავლების დაქვეითებას უკმაყოფილო მომხმარებლებისა და ორგანიზაციების რაოდენობის გაზრდისას [6].

5. უარყოფითი შედეგების შერბილების სტრატეგია

BGP დაუცველობის აღმოფხვრა მოითხოვს ტექნიკური, ოპერატიული და უსაფრთხოების პოლიტიკის ზომების ერთობლიობას [7-9].

- **რესურსების საჯარო გასაღების ინფრასტრუქტურა (RPKI):** RPKI ეხმარება BGP პროტოკოლის ანონსების ავთენტურობის დადასტურებას, რაც ამცირებს მარშრუტის გატაცების რისკს.
- **მარშრუტის ფილტრაცია და დადასტურება:** ქსელის ადმინისტრატორებს შეუძლიათ მარშრუტების ფილტრების დანერგვა პოტენციურად მავნე მარშრუტების დასაბლოკად და BGP ანონსების დასადასტურებლად.
- **BGP მონიტორინგი:** BGP მარშრუტების რეგულარული მონიტორინგი საშუალებას იძლევა ქსელის უსაფრთხოების სპეციალისტებმა რეალურ დროში აღმოაჩინონ ანომალიები და პოტენციური თავდასხმები.
- **BGP პარტნიორის აუთენტიფიკაცია (Peer Authentication):** BGP სესიების დაცვა ისეთი მექანიზმებით, როგორიცაა TCP MD5 ხელმოწერები ან ტრანსპორტის ფენის უსაფრთხოება (TLS).
- **პრეფიქსის გაფილტვრა:** ქსელის უსაფრთხოების ადმინისტრატორებმა აუცილებლად უნდა გამოიყენონ ფილტრაციის ტექნიკა ზედმეტად სპეციფიკური პრეფიქსების გავრცელების თავიდან ასაცილებლად.
- **კოორდინაცია:** ქსელის ოპერატორებს, ISP-ებს და ინტერნეტის მართვის ორგანიზაციებს შორის მუდმივი კომუნიკაცია, ერთობლივი ძალისხმევა გადამწყვეტია საუკეთესო პრაქტიკის შემუშავებისა და განხორციელებისთვის BGP პროტოკოლის უსაფრთხოებისათვის [10].

6. დასკვნა

მიუხედავად იმისა, რომ BGP პროტოკოლი მხარს უჭერს თანამედროვე ინტერნეტის ფუნქციონირებას, მისი დაუცველობა ქსელს მნიშვნელოვან რისკებს აყენებს. ინტერნეტის დინამიური და ურთიერთდაკავშირებული ბუნებიდან გამომდინარე რთულია ყველა დაუცველობის აღმოფხვრა, მაგრამ ინდუსტრიის ერთობლივი ძალისხმევით, უსაფრთხოების ზომებისა და სტანდარტების განხორციელებით, შეიძლება მნიშვნელოვნად შემსუბუქდეს BGP შეტევებთან დაკავშირებული რისკები. მუდმივი სიფხიზლე, თანამშრომლობა და განვითარებადი ტექნოლოგიების მიღება სასიცოცხლოდ მნიშვნელოვანია BGP ინფრასტრუქტურის გასაძლიერებლად და გლობალური ქსელის მუდმივი სტაბილურობისა და უსაფრთხოების უზრუნველსაყოფად.

ბიბლიოგრაფია

1. S. Kent, C. Lynn and K. Seo, "Secure Border Gateway Protocol (S-BGP)," in IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 582-592, April 2000, doi: 10.1109/49.839934.
2. G. Huston, M. Rossi and G. Armitage, "Securing BGP — A Literature Survey," in IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 199-222, Second Quarter 2011, doi: 10.1109/SURV.2011.041010.00041.
3. Iavich M., Iashvili G., Gnatyuk S., Tolbatov A., Mirtskhulava L. (2021) Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. In: Lopata A., Gudonienė D., Butkienė R. (eds) Information and Software Technologies. ICIST 2021. Communications in Computer and Information Science, vol 1486. Springer, Cham. https://doi.org/10.1007/978-3-030-88304-1_15
4. M. Caesar and J. Rexford, "BGP routing policies in ISP networks," in IEEE Network, vol. 19, no. 6, pp. 5-11, Nov.-Dec. 2005, doi: 10.1109/MNET.2005.1541715.
5. B. Al-Musawi, P. Branch and G. Armitage, "BGP Anomaly Detection Techniques: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 377-396, Firstquarter 2017, doi: 10.1109/COMST.2016.2622240.
6. Iavich, M. (2023). Post-quantum Scheme with the Novel Random Number Generator with the Corresponding Certification Method. In: Hu, Z., Wang, Y., He, M. (eds) Advances in Intelligent Systems, Computer Science and Digital Economics IV. CSDEIS 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 158. Springer, Cham. https://doi.org/10.1007/978-3-031-24475-9_7
7. Mitseva, Asya, Andriy Panchenko, and Thomas Engel. "The state of affairs in BGP security: A survey of attacks and defenses." Computer Communications 124 (2018): 45-60.
8. Butler, K., Farley, T. R., McDaniel, P., & Rexford, J. (2009). A survey of BGP security issues and solutions. Proceedings of the IEEE, 98(1), 100-122.
9. K. Butler, T. R. Farley, P. McDaniel and J. Rexford, "A Survey of BGP Security Issues and Solutions," in Proceedings of the IEEE, vol. 98, no. 1, pp. 100-122, Jan. 2010, doi: 10.1109/JPROC.2009.2034031.
10. Iavich, M., Gnatyuk, S., Iashvili, G., Odarchenko, R., Simonov, S. (2023). 5G Security Function and Its Testing Environment. In: Faure, E., Danchenko, O., Bondarenko, M., Tryus, Y., Bazilo, C., Zaspa, G. (eds) Information Technology for Education, Science, and Technics. ITEST 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 178. Springer, Cham. https://doi.org/10.1007/978-3-031-35467-0_39