Universitatea Tehnică a Moldovei

Analiza vulnerabilităților de securitate ale protocolului BGP

Masterand:
Bruma Ruslan

Conducător:
conf. univ., dr. Moraru Victor

Chișinău, 2020

Ministerul Educației, Culturii Și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei
FACULTATEA Calculatoare, Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susținere
Șef departament: conf.univ., dr
Fiodorov Ion,

_____

"__"_____2020

Analiza vulnerabilităților de securitate ale protocolului BGP

Teză de master în
Securitatea Informațională

Masterand: Bruma Ruslan
SI-191M
Conducător: Moraru Victor
conf.univ., dr

Chișinău, 2020

ADNOTARE

Teza cu titlul "Analiza vulnerabilităților de securitate ale protocolului Border Gateway Protocol (BGP) " elaborată de către Bruma Ruslan, în cadrul instituției Univeristatea Tehnică a Moldovei, este scrisă în limba Română și este constituită din 55 de pagini, 30 de figuri și 5 tabele. Structura tezei include: introducere, 3 capitole și concluzii.

Scopul lucrării este de a analiza totalitatea tehnicilor de securitate propuse pentru protocolul BGP și de a identifica metodele optime care pot fi implementate în producție la etapa actuală. De asemenea, această lucrare vine să încurajeze persoanele ce activează în domeniu să implementeze politicile de securitate pentru a proteja Internetul.
Internetul este o ierarhie de rețele interdependente între ele după anumite principii și criterii. Ca să asigurăm un nivel înalt de securitate a funcționării Internetului, este necesar sa stimulăm și să promovăm toate tehnicile noi de securitate care apar în prezent. Implementarea RPKI reprezintă una din cele mai bune practici pe care le avem la momentul de față și implementarea lui pe scară largă va spori semnificativ robustețea Internetului.

În teză au fost analizate studiile de specialitate făcute de-a lungul timpului asupra îmbunătățirii protocolului BGP. S-a facut o sinteză asupra metodelor propuse și s-a identificat metodele optime care pot fi ușor implementate la etapa actuală fără ca funcționarea Internetului să fie afectată.

În partea aplicativă a tezei s-a implementat framework-ul RPKI într-o rețea simulată asemănătoare cu o topologie reală. S-a demonstrat eficacitatea implementării RPKI pentru prevenirea atacurilor de deturnare a prefixelor.

ADNOTATION

The thesis entitled "Analysis of security vulnerabilities of the Border Gateway Protocol (BGP)" developed by Bruma Ruslan, within the Technical University of Moldova, is written in Romanian language and consists of 55 pages, 30 figures and 5 tables. The structure of the thesis includes: introduction, 3 chapters and conclusions.

The aim of the thesis is to analyze all the security techniques proposed for the BGP protocol and to identify the optimal methods that can be implemented in production at the current stage. This thesis also encourages people, working in the field, to implement security policies to protect the Internet.

Internet represent a hierarchy of networks interdependent with each other according to certain principles and criteria. In order to ensure a high level of security of the functioning of the Internet, it is necessary to stimulate and promote all the new security techniques that are currently emerging. The implementation of the RPKI is one of the best practices we have at the moment and its widespread implementation will significantly increase the robustness of the Internet.

The thesis analyzed the specialized studies done over time on improving the BGP protocol. A synthesis was made on the proposed methods and the optimal methods were identified that can be easily implemented at the current stage without affecting the functioning of the Internet.

In the application part of the thesis, the RPKI framework was implemented in a simulated network similar to a real topology. The effectiveness of the RPKI implementation for preventing prefix hijacking attacks has already been demonstrated.

CUPRINS

INTRODUCERE

Border Gateway Protocol (BGP) este protocolul care stă la baza funcționării Internetului. La etapa actuală, este un protocol nesigur cu potențial de propagare a informației false. În ultimul timp, tot mai des observăm probleme în funcționarea serviciului Internet datorită problemelor de securitate a protocolului BGP. În literatura de specialitate au fost prezentate mai multe măsuri de securitate pentru BGP, cu toate acestea, niciuna nu a fost adoptată până acum și, ca urmare, asigurarea securității BGP rămâne o problemă nerezolvată până în prezent.

Printre propunerile de securitate BGP existente, modelul Secure BGP (S-BGP) este considerat modelul care acoperă în mare parte, toate problemele de securitate. Cu toate acestea, implementarea acestui model impune provocări semnificative în ceea ce privește numărul mare de signaturi ce trebuie să fie verificate cât și considerații de implementare. Pentru ca acest model să ofere securitate cuprinzătoare, este necesar ca toate sistemele autonome (AS) din Internet să adopte acest model și să participe la adăugări de semnături și verificări în mesajele BGP. Anume ascest aspect stopează implementarea modelului S-BGP.

Un prim pas în implementarea S-BGP ar fi implementarea framework-ului RPKI. RPKI rezolvă parțial problemele de securitate a protocolului BGP, de asemenea, rezolvă o problemă majoră și anume “prefix hijacking”. În partea aplicativă a tezei este prezentată implementarea framework-ului RPKI și este simulat cazul “Verizon leak” din 24 iunie 2019 și este implementat frameworkul RPKI pentru a demonstra rezolvarea problemei aparute.

CONCLUZII GENERALE ȘI RECOMANDĂRI

Analizând tehnicile care au fost propuse pentru a securiza protocolul BGP, observăm că puține din ele au ajuns să fie implementate în producție. Problemele majore ale protocolului BGP ramân aceleași: integritatea hop-ului, autentificarea originii și validarea căii. Orice propunere pentru asigurarea securității BGP trebuie să permită implementarea treptată și trebuie să adauge doar modificări incrementale.

La etapa actuală nu a fost identificată o tehnică care ar rezolva cele trei probleme de bază ale protocolului. Cea mai optimă și ideală soluție ar fi implementarea tehnicii BGPsec, însă BGPsec este greu de implementat treptat și necesită resurse semnificative.

Odată cu sporirea resurselor echipamentelor de rețea, BGPsec este candidatul numărul 1 pentru a deveni un standard. Însă este irațional să așteptăm să fie implementată o tehnică de securizare ideală, securitatea trebuie aplicată astăzi.

La etapa actuală un mecanism simplu de implementat este frameworkul RPKI care ne rezolvă problema autentificării originii. Avantajul acestei tehnici este că implementarea se poate face independent față de alte sisteme autonome. Alt avantaj al tehnicii în cauză este că aceasta nu mărește timpul de convergență al tabelei de rutare, iar acest lucru se datorează faptului că mesajele BGP nu sunt îngreunate cu informații criptate, iar validarea rutelor se face prin consultarea unei baze de date locale.

Din punct de vedere statistic, 15% din totalitatea sistemelor autonome sunt de tip tranzit. Dacă ar fi aplicată tehnica RPKI în cele 15% din toate sistemele autonome, am putea spune ca problema legată de autentificarea originii este rezolvată. Însă realitatea ne arată că mulți operatori mari precum: Verizon, Rostelecom, s.a., nu implementează tehnici elementare de securitate astfel lasând Internetul vulnerabil.

Din punct de vedere al autorului, motivul din cauza căruia operatorii Tier-1 nu au implementat RPKI-ul este de tip economic. Dacă operatorii mari nu vor accepta prefixele fara ROA, traficul de tranzit se va reruta prin alți operatori care nu au filtre bazate pe ROA, astfel traficul va ocoli propriul AS. Într-un final putem afirma că atâta timp cât tehnicile de securizare a protocolului BGP nu vor fi obligatorii, Internetul va ramâne vulnerabil și lucrurile nu se vor schimba spre bine.

BIBLIOGRAFIE

1. CISCO PRESS, *BGP Basics: Internal And External BGP*, 2017 [Online] [citat 23 septembrie 2020] Disponibil: https://www.networkcomputing.com/data-centers/bgp-basics-internal-and-external-bgp
2. NOCTION, *Understanding the AS path and AS path prepending*, 2015 [Online] [citat 23 septembrie 2020] Disponibil: https://www.noction.com/blog/as-path-and-as-path-prepending
3. LI Q., HU Y., ZHANG X., *Even Rockets Cannot Make Pigs Fly Sustainably Can BGP be Secured with BGPsec, ETH Zurich, 2014.* [Online] [citat 28 septembrie 2020] Disponibil: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/86415/eth-8844-01.pdf
4. SMITH B. R., GARCIA-LUNA-ACEVES J. J., *Securing the border gateway routing protocol*. " in Proc., Global Internet '96, 1996, p. 81–85. [citat 3 octombrie 2020]
5. PERLMAN R. J., *Network layer protocols with byzantine robustness*, Ph.D. Dissertation, Massachusetts Institute of Technology, 1988. [citat 3 octombrie 2020]
6. KUMAR B., *Integration of security in network routing protocols*, ACM SIGSAC Review, vol. 11, no. 2, 1993, p 18–25. [citat 6 octombrie 2020]
7. CHEUNG S., *An efficient message authentication scheme for link state routing*, in Proc., 13th Annual Computer Security Applications Conference, 1997, p. 90–98.
8. HEFFERMAN A., *Protection of BGP sessions via the TCP MD5 signature option*, IETF, RFC 2385, 1998. [citat 8 octombrie 2020]
9. AIELLO W., IOANNIDIS J., MCDANIEL P., *Origin authentication in interdomain routing*, Proc., 10th ACM conference on Computer and Communications Security, 2003, p. 165–178 [citat 18 octombrie 2020]
10. SUBRAMANIAN L., ROTH V., STOICA I., SHENKER S., KATZ R., *Listen and whisper: Security mechanisms for BGP*, in Proc., NSDI, 2004 [citat 21 octombrie 2020]
11. HU Y. C., PERRIG A., SIRBU M., *SPV: secure path vector routing for securing BGP*, in Proc., ACM SIGCOMM, 2004, p. 179–192. [citat 28 octombrie 2020]
12. BUTLER K., AIELLO W., *Optimizing BGP security by exploiting path stability*, Proceedings of the 13th ACM conference on Computer and communications security, 2006, p. 298–310. [citat 28 octombrie 2020]
13. HC-BGP: A Light-weight and Flexible Scheme for Securing Prefix Ownership [citat 3 noiembrie 2020]

14. BRADLEY K. A., CHEUNG S., PUKETZA N., MUKHERJEE B., OLSSON R. A., *Detecting disruptive routers: a distributed network monitoring approach*, in Proc., IEEE Symposium on Security and Privacy, IEEE Network, vol. 12, 1998, p. 50–60 [citat 14 octombrie 2020]
15. ZHAO X., WANG D., WANG L., MASSEY D., MANKIN A., WU S. F., ZHANG L., *Validation of the multiple origin ASes conflicts through BGP community attribute*, IETF Draft, 2001. [citat 12 noiembrie 2020]
16. KRUEGEL C., MUTZ D., ROBERTSON W., VALEUR F., *Topology-based detection of anomalous BGP messages*, in Proc., Symposium on Recent Advances in Intrusion Detection, 2003 [citat 14 noiembrie 2020]
17. WAN T., KRANAKIS E., VAN OORSCHOT P. C., *Pretty secure BGP (psBGP)*, School of Computer Science, Carleton University, Tech. Rep., 2005. [citat 16 noiembrie 2020]
18. KARLIN J., FORREST S., REXFORD J., *Pretty good BGP: Improving BGP by cautiously adopting routes*, in Proc., International Conference on Network Protocols, 2006. [citat 20 noiembrie 2020]
19. BLAZAKIS D., BARAS J. S., *Analyzing BGP ASPATH behavior in the Internet*, in Proc., 9th IEEE Global Internet Symposium, 2006. [citat 22 noiembrie 2020]
20. QIU J., GAO L., *Hi-BGP: A lightweight hijack-proof inter-domain routing protocol*, Department of ECE, University of Massachusetts, Tech. Rep., 2006. [citat 3 octombrie 2020]
21. HU X., MAO Z., *Accurate Real-time Identification of IP Prefix Hijacking*, IEEE Symposium on Security and Privacy, 2007, p. 3–17. [citat 25 noiembrie 2020]
22. ZHANG Z., ZHANG Y., HU Charlie Y., MORLEY Mao Z., Bush R., *iSPY: Detecting IP Prefix Hijacking on My Own*, ACM SIGCOMM HotNets Workshop, vol. 2006 [Online]. Disponibil: http://ccr.sigcomm.org/online/files/p327-zhangA.pdf [citat 28 noiembrie 2020]
23. REYNOLDS P., KENNEDY O., SIRER E. G., SCHNEIDER F. B., *Securing BGP using external security monitors*, Cornell University, Tech. Rep., 2006 [citat 29 noiembrie 2020]
24. WENDLANDT D., AVRAMOPOULOS, ANDERSEN D., REXFORD J., *Don't secure routing protocols, secure data delivery*, ACM SIGCOMM HotNets Workshop, vol. 2006. [Online]. Disponibil: http://www.cs.princeton.edu/jrex/papers/acr.pdf [citat 24 septembrie 2020]
25. LAD M., MASSEY D., PEI D., WU Y., ZHANG B., ZHANG L., *PHAS: A Prefix Hijack Alert System*, Proc. Of USENIX Security symposium, 2006. [citat 18 noiembrie 2020]
26. LAD M., MASSEY D., WU Y., ZHANG B., ZHANG L., *PHAS: A prefix Hijack Alert System*, 2006. [Online] [citat 5 noiembrie 2020] Disponibil: https://www.usenix.org/legacy/event/sec06/tech/full_papers/lad/lad_html/originChange.html

27. LIAO Y., GAO L., GUERIN A.R., ZHANG Z., *Inter-domain routing under diverse commercial agreements, IEEE Xplore*, January 2011. [citat 24 noiembrie 2020]
28. BALLANI H., FRANCIS P., ZHANG X., *A study of prefix hijacking and interception in the Internet,* ACM SIGCOMM 2007 Data Communications Festival, 2007. [citat 8 octombrie 2020]
29. HALEVI S., GOLDBERG S., JAGGARD A.D., WRIGHT R.N., *Rationality and traffic attraction: Incentives for honest path announcements in BGP,* Proceedings of the ACM SIGCOMM 2008 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, January 2008. [citat 10 septembrie 2020]
30. MCARTHUR C., GUIRGUIS M., *Stealthy IP Prefix Hijacking: Don't Bite Off More Than You Can Chew,* Global Telecommunications Conference, 2009. [citat 12 noiembrie 2020]
31. GOLDBERG S, SCHAPIRA M., HUMMON P., REXFORD J., *How secure are secure interdomain routing protocols, Computer Networks,* 9 September 2014, vol 70, p. 260-287. [citat 13 octombrie 2020]
32. SHUE C.A., KALAFUT A., GUPTA M., *Abnormally Malicious Autonomous Systems and Their Internet Connectivity, IEEE Xplore,* March 2012. [citat 12 s 2020]
33. KIHONG P., HEEJO L., *On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets, Computer Communication Review,* 2001, vol 31, p. 15-26.
34. RPKI, *RPKI Technology,* 2018. Disponibil: https://rpki.readthedocs.io/en/latest/rpki/introduction.html [citat 24 septembrie 2020]
35. GOODELL G., AIELLO W., GRIFFIN T., IOANNIDIS J., MCDANIEL P., RUBIN A., *Working around BGP: An incremental approach to improving security and accuracy of interdomain routing*. In Proceedings of the Network and Distributed System Security Symposium (ISOC NDSS'03), Feb. 2003, p. 75–85. [citat 14 noiembrie 2020]