HAL open science

Emulation on the Internet Prefix Hijacking Attack Impaction

Jinjing Zhao, Yan Wen

To cite this version:

Jinjing Zhao, Yan Wen. Emulation on the Internet Prefix Hijacking Attack Impaction. 1st International Conference on Information and Communication Technology (ICT-EurAsia), Mar 2013, Yogyakarta, Indonesia. pp.485-489, 10.1007/978-3-642-36818-9_54 . hal-01480207

HAL Id: hal-01480207

https://inria.hal.science/hal-01480207

Submitted on 1 Mar 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Emulation on the Internet Prefix Hijacking Attack Impaction

Jinjing Zhao[1,2], Yan Wen[1,2]

[1]Beijing Institute of System Engineering,Beijing, China
[2]National Key Laboratory of Science and Technology on Information System Security, Beijing, China

misszhaojinjing@hotmail.com
celestialwy@gmail.com

Abstract. There have been many incidents of IP prefix hijacking by BGP protocol in the Internet. Attacks may hijack victim's address space to disrupt network services or perpetrate malicious activities such as spamming and DoS attacks without disclosing identity. The relation between network topology and prefix hijacking influence is presented for all sorts of hijacking events in different Internet layers. The impaction parameter is analyzed for typical prefix hijacking events in different layers. A large Internet emulation environment is constructed and the attack impaction of IP prefix hijacking events are evaluated. The results assert that the hierarchical nature of network influences the prefix hijacking greatly.

Keywords: IP prefix hijacking; Power law; BGP; Inter-domain routing system; Internet emulation environment.

1 Instruction

Prefix hijacking is also known as BGP hijacking, because to receive traffic destined to hijacked IP addresses, the attacker has to make those IP addresses known to other parts of the Internet by announcing them through BGP. Because there is no authentication mechanism used in BGP, a mis-behaving router can announce routes to any destination prefix on the Internet and even manipulate route attributes in the routing updates it sends to neighboring routers. Taking advantage of this weakness has become the fundamental mechanism for constructing prefix hijack attacks. They occur when an AS announces a route that it does not have, or when an AS originates a prefix that it does not own.

Previous efforts on prefix hijacking are presented from two aspects: hijack prevention and hijack detection. Generally speaking, prefix hijack prevention solutions are based on cryptographic authentications [4-8] where BGP routers sign and verify the origin AS and AS path of each prefix. While hijack detection mechanisms [9-15] are provided when a prefix hijack is going to happening which correction steps must follow. Because there is a lack of a general understanding on the impact of a successful

prefix hijack, it is difficult to assess the overall damage once an attack occurs, and to provide guidance to network operators on how to prevent the damage.

In this paper, we conduct a systematic study on the impaction prefix hijacks launched at different position in the Internet hierarchy. The Internet is classified into three hierarchies—core layer, forwarding layer and marginal layer based on the commercial relations between autonomous systems (ASes). And a large Internet emulation environment is constructed which hybridizes the network simulation technology and packet-level simulation technology to achieve a preferable balance between fidelity and scalability. The experiment results show that the hierarchical nature of network influences the prefix hijacking greatly.

The remainder of this paper is organized as follows: The related works are discussed in section 2. The impaction analysis of the prefix hijacks attack is presented in section 3, in which IP prefix hijacks are classified on a comprehensive attack taxonomy relying on the Internet hierarchy model and BGP protocol policies. Section 4 builds an emulation environment to test the correctness of our conclusion and section 5 concludes the paper.

2 Related work

Various prefix hijack events have been reported to NANOG [19] mailing list from time to time. IETF's rpsec (Routing Protocol Security Requirements) Working Group provides general threat information for routing protocols and in particular BGP security requirements [20]. Recent works [3,21] give a comprehensive overview on BGP security. The prefix hijacking is one of the key problems being noticed to BGP in these papers.

Previous works on prefix hijacking can be sorted into two categories: hijack prevention and hijack detection. The former one is trying to prevent the hijacking in the protocol mechanism level, and the latter one is trying to find and alert the hijacking event after it happening. The methods adopted can be categorized into two types: cryptography based and non-crypto based.

3 Analysis on Prefix Hijack Attack Impaction

3.1 Internet Hierarchy

In [18], we build a three-hierarchy model of the Internet and give an efficient arithmetic for it. The model is organized as follows:

a) The set of nodes who have no providers forms a clique (interconnection structure), which is the core layer.

b) If the nodes don’t forward data for others, then it belongs to the marginal layer.

c) The node that belongs to neither the core layer nor the marginal layer belongs to the forwarding layer. And the forwarding layer has several sub-layers.

3.2 The relation between prefix hijacking and the Internet Hierarchy

For the simpleness of the description, the ASes whose prefixes being hijacked are expresses with V, and the hijack attack ASes are denoted by A. Furthermore, we suppose each AS only has one provider. The multi-home mechanism is not considered in this paper.

To evaluate the influence if prefix hijacking events, two impaction parameters are introduced as follows:

Definition 1 Set of the affected nodes *Nc*: The set of nodes whose routing states might be changing because of the happening prefix hijacking event.

Definition 2 Affected path factor μ: The percentage of the paths might be changed because of the happening prefix hijacking event.

In paper [23],we classified the prefix hijacking events into nine types according to the different positions which the attackers and victims are located. The relation between prefix hijacking and the Internet hierarchy are concluded by the two impaction parameters .

From the analysis, these results can be drawn:

1) The hijacked AS in the core layer is not the most awful thing. On the contrary, if the AS in the marginal layer being hijacked, the number of the affected nodes is the largest among the three levels;

2) The hijacked AS in the forwarding layer can affect more paths than the core layer or the marginal layer;

3) If the hijacked ASes are in the same level, the hijacking AS in the forwarding layer can affect more nodes than the core layer or the marginal layer, and the higher attacker is in, the larger its influence will be;

4) The sub-prefix hijack can affect more ASes than the same prefix hijack, and the lager sub-prefix range is, the bigger affected path factor μ will be.

4 Evaluation Environment and Experiment

In order to verify the correctness of the conclusions in section 3, we build a prefix hijacking attack emulation environment, which is composed of three Juniper J2350 routers and four server computers. Each server can emulate 30 virtual routers.

For the authenticity of the test, the real BGP data is samples for the topology of inter-domain system. According to the sampling rules in [22], a network with 110 ASes is build, and the commercial relations are reserved. The network is also be classified into layers by the hierarchical algorithm in section 3.

Each prefix hijacking cases, we repeat the attach process three times, and calculate the average values of the affected nodes number *Nc* and path factor μ. The results are described in Table 1.

From the expariment results, we can see that if the AS in the marginal layer being hijacked, the number of the affected nodes is the largest among the three levels; the hijacked AS in the forwarding layer can affect more paths than the core layer or the marginal layer; and the hijacking AS in the forwarding layer can affect more nodes than the core layer or the marginal layer.

Table 1. Experiment Results

Case	*Nc*	*μ*
V∈C, A∈C	13	43
V∈C, A∈F	24	53
V∈C, A∈S	18	36
V∈F, A∈C	28	118
V∈F, A∈F	34	78
V∈F, A∈S	21	62
V∈S, A∈C	32	75
V∈S, A∈F	57	73
V∈S, A∈S	28	65

5 Conclusion

This paper conducts a systematic study on the impaction prefix hijacks launched at different position in the Internet hierarchy based on the work in paper [23]. A large Internet emulation environment is constructed which hybridizes the network simulation technology and packet-level simulation technology to achieve a preferable balance between fidelity and scalability. The experiment results show that the hierarchical nature of network influences the prefix hijacking greatly.

Acknowledgment

This research is supported by National Natural Science Foundation of China (Grant No. 61100223).

References

1. Mohit Lad, Ricardo Oliveira, Beichuan Zhang and Lixia Zhang ,Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks. pp.368-377, 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07), 2007.
2. O. Nordstrom and C. Dovrolis, Beware of BGP attacks, SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, 2004.
3. Kevin Butler, Patrick McDaniel and Jennifer Rexford. A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE. Vol. 98, No. 1, January 2010
4. L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. H. Katz. Listen and whisper: Security mechanisms for BGP. In Proceedings of ACM NDSI 2004, March 2004.
5. J. Ng. Extensions to BGP to Support Secure Origin BGP. ftp://ftp-eng.cisco.com/sobgp/drafts/draft-ng-sobgpbgp-extensions-02.txt, April 2004.
6. S. Kent, C. Lynn, and K. Seo. Secure border gateway protocol (S-BGP). IEEE JSAC Special Issue on Network Security, 2000

7. S. S. M. Zhao and D. Nicol. Aggregated path authentication for efficient bgp security. In 12th ACM Conference on Computer and Communications Security (CCS), November 2005.
8. B. R. Smith, S. Murphy, and J. J. Garcia-Luna-Aceves. Securing the border gateway routing protocol. In Global Internet' 96, November 1996.
9. RIPE. Routing information service: myASn System. http://www.ris.ripe.net/myasn.html.
10. M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang. PHAS: A prefix hijack alert system. In 15th USENIX Security Symposium, 2006.
11. S. Qiu, F. Monrose, A. Terzis, and P. McDaniel. Efficient techniques for detecting false origin advertisements in interdomain routing. In Second workshop on Secure Network Protocols (NPSec), 2006.
12. J. Karlin, S. Forrest, and J. Rexford. Pretty good bgp: Protecting bgp by cautiously selecting routes. Technical Report TR-CS-2005-37, University of New Mexico, Octber 2005.
13. W. Xu and J. Rexford. MIRO: multi-path interdomain routing. In SIGCOMM 2006, pages 171–182, 2006.
14. X. Hu and Z. M. Mao, Accurate Real-time Identification of IP Prefix Hijacking, in Proc. of IEEE Security and Privacy (Oakland), 2007.
15. C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Realtime, in Proc. of ACM SIGCOMM, August 2007.
16. R. Govindan and A. Reddy. An Analysis of Internet Inter-Domain Topology and Route Stability. In Proc. IEEE INFOCOM '97, March 1997.
17. GE Z, FIGUEIREDO D, JAIWAL S, and et al. On the hierarchical structure of the logical Internet graph [A]. Proceedings of SPIE ITCOM[C]. USA, August 2001.
18. Peidong Zhu, Xin Liu. An efficient Algorithm on Internet Hierarchy Induction. High Technology Communication.14: 358-361, 2004.
19. The NANOG Mailing List. http://www.merit.edu/mail.archives/nanog/.
20. B. Christian and T. Tauber. BGP Security Requirements. IETF Draft: draft-ietf-rpsec-bgpsecrec-04, March 2006.
21. Sharon Goldberg, Michael Schapira, Peter Hummon, Jennifer Rexford. How Secure are Secure Interdomain Routing Protocols? in Proc. of ACM SIGCOMM, August 30–September 3, 2010, New Delhi, India.
22. http://www.ssfnet.org/Exchange/gallery/asgraph/src.tar.gz
23. Zhao JJ, Wen Yan, Li Xiang, etc. The Relation on Prefix Hijacking and the Internet Hierarchy, The 6th International Conference on Innovative Mobile and Internet Services (IMIS'12), Italy, July, 2012.
24. Shuyuan Mary Ho and Hwajung Lee. A Thief among Us: The Use of Finite-State Machines to Dissect Insider Threat in Cloud Communications. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). Volume 3, Number 1/2 (March 2012).
25. Yoshiaki Hori, William Claycomb, and Kangbin Yim. Guest Editorial: Frontiers in Insider Threats and Data Leakage Prevention. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). Volume 3, Number 1/2 (March 2012).
26. Sang Min Lee and Dong Seong Kim and Jong Sou Park. A Survey and Taxonomy of Lightweight Intrusion Detection Systems. Journal of Internet Services and Information Security. Volume 2, Issue 1/2, February 2012