Measuring and Analyzing on Effection of BGP Session Hijack Attack

ZHAO JINJING[1,2], LI YUANLING[1,2], LIU LI[1,2]
[1]National Key Laboratory of Science and Technology on Information System Security
[2]Beijing Institute of System and Engineering
P.O.box 9702-19, Beijing, CHINA
misszhaojinjing@hotmail.com liyuanling@bbn.cn liuli_sunny@163.com

Abstract: - 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. The relation of network topology and prefix hijacking influence is presented for all sorts of hijacking events in different Internet layers. And a large Internet emulation environment is constructed and the attack impaction of IP prefix hijacking events are evaluated. The results that the hierarchical nature of network influences the effection of the BGP hijacking attack greatly.

Key-Words: - BGP hijacking; Inter-domain routing system; Internet emulation environment.

1 Introduction

BGP session hijacking is also known as prefix 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.

Prefix hijacking can happen in one of three ways - a block containing unallocated space can be announced, a sub-block of an existing allocation can be announced, or a competing announcement for exactly the same space as an existing allocation can be announced. Upon receiving these fabricated advertisements, other BGP routers may be fooled into thinking that a better or more specific route has become available towards the target prefix and start forwarding future traffic along the false path. As a result of the prefix hijacking, part (if not all) of the traffic addressed to the target prefix will be forwarded to the attacker instead of the target prefix. 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 of 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 [23] 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 [24]. Recent works [3,25] 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 formal 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 which adopted can be categorized into two types: cryptography based and non-crypto based.

The cryptography methods, like [4-6, 27-31], that BGP routers sign and verify the origin AS and AS path of each prefix. Origin authentication [31] uses trusted database to guarantee that an AS cannot falsely claim to be the rightful owner for an IP prefix. However, the manipulator can still get away with announcing any path that ends at the AS that rightfully owns the victim IP prefix. Secure Origin BGP (soBGP) [30] provides origin authentication as well as a trusted database that guarantees that any announced path physically exists in the AS-level topology of the internetwork. However, a manipulator can still get away with announcing a path that exists but is not actually available. In addition to origin authentication, S-BGP [6] also uses cryptographically-signed routing announcements to provide a property called path verification. It effectively limits a single manipulator to announcing available paths. However, S-BGP does not prevent the manipulator from announcing the shorter, more expensive, provider path, while actually forwarding traffic on the cheaper, longer customer path. In SPV [32], the originator of a prefix establishes a single root value used to seed the generation of one-time signature structures for each hop in the PATH. However, the security of SPV is in some cases based on probabilistic arguments, which may be acceptable for some constrained environments, and it is unclear whether such arguments will be acceptable in the larger Internet. And it does not provide the requisite security to protect against path modification. In addition to added router workload, these solutions require changes to all router implementations, and some of them also require a public key infrastructure. Due to these obstacles, none of the proposed prevention schemes is expected to see deployment in near future.

The non-crypto methods include [4, 9, 10, 12, 14]. PHAS [10] is predicated on the notion that a prefix owner is the only entity that can differentiate between real routing changes and those that take place as a result of a prefix hijacking attack. And if there are changes to the originator of a route, the owner of that prefix is notified through email. The system is incrementally deployable in that to join the system. A prefix owner need only register with the PHAS server; however, this server is also a single point of failure in the system, and if it is compromised, it could send out numerous false alarms to prefix owners. Additionally, the system relies on the validity of entities registering their prefixes; there is no protection against an adversary making a false registration. Hu and Mao examined prefix hijacking in greater detail and provided a mechanism for detecting prefix hijacking attacks in real time [14]. Their solution is based on fingerprinting techniques for networks and hosts. If there are conflicting origin ASes advertised, which is potential evidence of a prefix hijacking attack, the collected fingerprints are compared against probes sent to all origins. This approach relies on a real-time BGP UPDATE monitor, which sends differentiating probes if prefixes are advertised from multiple locations. The availability of the monitor is critical as, if updates are delayed, the ability to collect measures, such as probing and subsequent decision making, will be compromised. The Whisper protocol [4] is designed to validate the initial source of path information. The protocol seeks to alert network administrators of potential routing inconsistencies. A random value is initially assigned to each prefix by the originator. The value is repeatedly hashed at each hop as it is propagated from AS to AS. if the hash values are the same, then they must have come from the same source. Only the route originator can verify the route because of the non-invertibility of secure hash functions. Thus, the recipient would have to query the originator as to the veracity of the route, which is often outside of the purview of the originator’s knowledge. Another recently-proposed alerting system is pretty good BGP (PGBGP) [12]. The key insight in this work is that misconfigurations and prefix hijacking attacks could be mitigated if routers exercise a certain amount of judgement with the routes that they adopt into their routing tables. MyASN[9] is an offline prefix hijack alert service provided by RIPE. A prefix owner registers the valid origin set for a prefix, and MyASN sends an alarm via regular email when any invalid origin AS is observed in BGP routing update.

ISBN: 978-960-474-310-0

3 Analysis on Prefix Hijack Attack Impaction

3.1 Internet Hierarchy

Paper[20] presents a hierarchical formalization method for Internet. In [21], a five-hierarchy model of the Internet is presented based on the commercial relation between ASes. These models are too complex to analyze for BGP convergence. In [22], we build a three-hierarchy model of the Internet and give an efficient algorism 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.

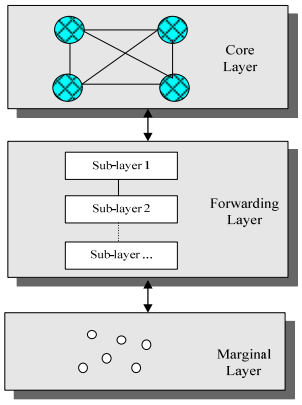

Fig. 1. Three-Hierarchy Model of the Internet

3.2 The relation on prefix hijacking and the Internet Hierarchy

The systematic study on the impaction of prefix hijacks launched at different position in the Internet hierarchy is descripted in this part, after the Internet hierarchy model and the prefix hijacking type are cleared.

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 [34],we classified the prefix hijacking events into nine types according to the different positions which the attackers and victims are located(shown in Fig.2). The relation on 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

4.1 Evaluation Environment Construction

In order to verified the correctness of our conclusion, an evaluation environment is constructed which hybridizes the network simulation technology and packet-level simulation technology to achieve a preferable balance between fidelity and scalability.

In the pointer of view of the experiment environment building technologies, varied feasible hybrid methods can be divided into two categories: the methods combining the packet-level simulation and analytical model, and the methods integrating the network simulation and packet level simulation. The experimental environments built with the hybrid methods combining the packet-level simulation and analytical model have good scalability and simulation efficiency, but fail to address the terminal simulation fidelity, nor the effective analysis and evaluation of prefix hijacking. The hybrid methods integrating the network simulation and packet-level simulation can not only have considerable scalability, the advantage of

ISBN: 978-960-474-310-0

packet-level simulation, but also hold high fidelity which just is the advantage of network simulation. Furthermore, it builds the experimental environments using the simulation idea of hardware-in-loop, thereby having the capability of directly interacting with the network equipment and software. Consequently, it can directly evaluate and analyze the impaction of prefix hijacking attack.

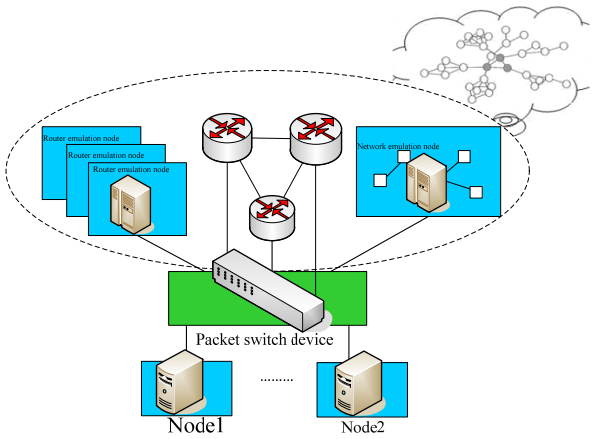

Fig. 2. Prefix Hijacking Evaluation Environment

Based on the analysis to different experimental environments building technologies, we can draw a conclusion that the hybrid methods combining the packet level simulation and network simulation hold obvious advantages in four aspects, viz., network characteristics, node characteristics, attack characteristics and experimental environment characteristics.

Fig.2 illustrates the structure of our prefix hijacking evaluation environment, which is composed of the emulation network and the emulation nodes. The emulation networks, , which can support the emulation of the topology structure of the network, conclude the network emulation nodes, router emulation nodes, security nodes, etc. the emulation nodes can support the emulation of the prefix hijacking attack mechanisms.

4.2 Prefix Hijacking Attack 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.

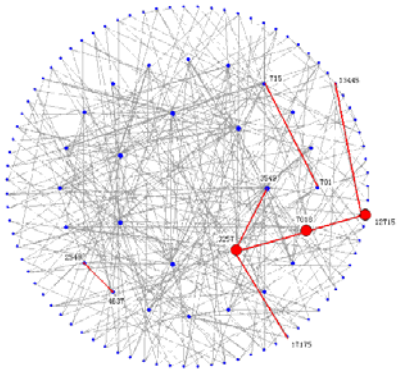

Fig. 3. Topology Graph of the Emulation Network

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 [33], 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. Fig.3 is the topology graph of the network.

Table 1 lists nine prefix hijacking attack cases in the emulation and the ID of the selected attack ASes and the victim ASes.

Table 1. Nine Types of the Experimental Preifix Hijacking Events

Case	Description	ID
V∈C, A∈C	**Victims in C, Attackers in C**	AS 3257->7518
V∈C, A∈F	**Victims in C, Attackers in F**	AS 3257->3549
V∈C, A∈S	**Victims in C, Attackers in S**	AS 3257->12715
V∈F, A∈C	**Victims in F, Attackers in C**	AS 7018->715
V∈F, A∈F	**Victims in F, Attackers in F**	AS 7018->701
V∈F, A∈S	**Victims in F, Attackers in S**	AS 7018->17175
V∈S, A∈C	**Victims in S, Attackers in C**	AS 12715->7518
V∈S, A∈F	**Victims in S, Attackers in F**	AS 12715->715
V∈S,	**Victims in S, Attackers**	AS 12715-

ISBN: 978-960-474-310-0

A∈S	**in S**	>17175

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 2.

Table 2. 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

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.

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 [34]. The Internet is classified into three hierarchies—core layer, forwarding layer and marginal layer based on the power-law and commercial relations of ASes. Two impaction parameters—affected ASes set Nc and affected paths factor μ, are analyzed for nine types of prefix hijacking events based on the position of the hijacking ASes and the hijacked ASes.

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] H. Ballani, P. Francis, and X. Zhang, *A Study of Prefix Hijacking and Interception in the Internet.* SIGCOMM Comput. Commun. Rev., vol. 37, no. 4, pp. 265–276, 2007.

[17] M. Lad, R. Oliveira, B. Zhang, and L. Zhang, *Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks*, in Proc. of IEEE/IFIP DSN, 2007.

[18] Michalis Faloutsos, Petros Faloutsos, Christos Faloutsos. *On Power-Law Relationships of the Internet Topology.*1999.

[19] Zegura, Calvert and Donahoo, *A quantitative comparison of graph-based models for Internet topology*, IEEE/ACM Transactions on Networking, December 1997.

[20] R. Govindan and A. Reddy. *An Analysis of Internet Inter-Domain Topology and Route Stability*. In Proc. IEEE INFOCOM ‘97, March 1997.

[21] GE Z, FIGUEIREDO D, JAIWAL S, and et al. *On the hierarchical structure of the logical Internet graph*. Proceedings of SPIE ITCOM. USA, August 2001.

[22] Peidong Zhu, Xin Liu. *An efficient Algorithm on Internet Hierarchy Induction*. High Technology Communication.14: 358-361, 2004.

[23] The NANOG Mailing List. http://www.merit.edu/mail.archives/nanog/.

[24] B. Christian and T. Tauber. *BGP Security Requirements*. IETF Draft: draft-ietf-rpsec-bgpsecrec-04, March 2006.

[25] 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.

[26] Y. Rekhter, T. Li, and S. Hares. *Border Gateway Protocol 4*. RFC 4271, Internet Engineering Task Force, January 2006.

[27] RFC 4271, *Internet Engineering Task Force*, January 2006. 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.

[28] B. R. Smith, S. Murphy, and J. J. Garcia-Luna-Aceves. *Securing the border gateway routing protocol*. In Global Internet’ 96, November 1996.

[29] T. Wan, E. Kranakis, and P. van Oorschot, *Pretty Secure BGP(psBGP)*, in Proc. of NDSS, 2005.

[30] R. White, *Architecture and Deployment Considerations for Secure Origin BGP (soBGP)*, draft-white-sobgp-architecture-01, Nov 2005.

[31] W. Aiello, J. Ioannidis, and P. McDaniel, *Origin authentication in interdomain routing*, in Proc. of conference on Computer and communications security (CCS), 2003.

[32] Y.-C. Hu, A. Perrig, and M. Sirbu, B. *SPV: Secure path vector routing for securing BGP*, in Proc. ACM SIGCOMM, Portland, OR, Aug. 2004.

[33] http://www.ssfnet.org/Exchange/gallery/asgraph/src.tar.gz

[34] 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.