On the Prevention of Invalid Route Injection Attack

Meng Li, Quanliang Jing, Zhongjiang Yao, Jingang Liu

On the Prevention of Invalid Route Injection Attack

Meng Li, Quanliang Jing, Zhongjiang Yao, Jingang Liu

Capital Normal University Haidian District, Beijing City,China

limeng7065@gmail.com;QuanliangJing@ict.ac.cn;
zhongjiangyao@163.com;liujg2003@163.com

ABSTRACT: In recent years, the Internet is suffering from severe attacks from the global routing system, such as prefix hijack, digital cannon. These attacks break down network services and sabotage infrastructures. In this paper, we present a novel attack on route control plane---invalid route injection, and simulate the attack by adding controlled software routers in the stub and check the resource consumptions of routers before and after the attack. The experimental results demonstrate that invalid route injection can bring severe damage to routers in the Internet. Based on the analysis of the results, we discuss the prevention of the attack and propose some effective protection and countermeasures to the attack.

KEYWORDS: invalid route; injection; OSPF;BGP; route attack.

1 Introduction

With the rapid development and growth of IP technology, Internet has penetrated into politics, economy, military and daily life and brought it a corresponding increased reliance on the underlying infrastructures. Therefore, it is essential to ensure the security of the Internet. Route security is an important part of Internet security. It is becoming vitally important and facing significant challenges at the same time.

The Internet is composed of tens of thousands of Autonomous Systems (ASes) which operate individual parts of the infrastructures. ASes exchange route information via an external gateway protocol like BGP [1] (Border Gateway Protocol). Within an AS, routers communicate with each other through intra-domain routing protocols [2] such as OSPF (Open Shortest Path First Protocol) which has been widely used currently, and IS-IS (Intermediate System to Intermediate System) which is developing and spreading gradually. These protocols can efficiently distribute dynamic topological information among its participants, facilitate route calculations and make packet forwarding decisions. They form the heart of Internet infrastructures.

However, these routing protocols are not so robust for their disadvantages and loopholes which can cause some incidents or be used by malicious attempts to compromise the availability of the network [3]. For example, since its own route information cannot be validated by BGP itself, it has to fully trust all the other peering routers[5]. Based on that, On 24th February 2008, Pakistan Telecom started an unauthorized announcement of prefix 208.65.153.0/24. PCCW Global, one of Pakistan Telecom's upstream providers, forwarded this announcement to the rest of the Internet, which resulted in the hijacking of YouTube traffic on a global scale [6]. For another, Max Schuchard, from the University of Minnesota in 2010 put forward the concept of 'digital cannon'[7], which showed that a digital cannon using a 'botnet' composed of 25000 computers can destroy the entire Internet using BGP protocol. These routing incidents result in irreparable damage to the politics and economics.

In order to detect the routing attacks effectively and provide a theoretical foundation for routing attack detection, in this paper we present a novel network routing attack named invalid route injection. Then we do some simulate experiments to verify the attack. The results show that the invalid route injection attacks do have an effect on the communication among the hosts or routers, causing a serious impact on the stability and security of the network. Finally we discuss some preventive measures.

2 Related Work

Using the control plane to attack the Internet has recently been proposed to the literature. 'Digital cannon', which interferes information exchange by using data plane to affect control plane, is one of such attacks. The attack causes routers frequently exchanging neighbor routing information, resulting in the exhaustion of CPU, memory and other resources of the routers, and eventually crushing control plane. However, this method needs to get the topology of the entire network and critical devices. Once the network devices filter the ICMP packets, the attack will not happen [8]. Currently, there are also many instances of 'prefix hijacking' attacks in the Internet, which are caused by mis-configuration of routing information or malicious attempts. The AS that hijacks a prefix can intercept all the hijacked traffic, result in a denial-of-service attack against the hijacked AS. Also the hijacks can redirect the traffic to an incorrect destination for phishing attack. Although prefix hijack has many cases in theory, it is hard to implement in reality since the Internet has not only very strict access strategy of the Internet, but also the attack need to configure the routes directly [9]. This paper introduces a new method of routing attack—invalid route injection attack. This methodology avoids directly manipulating core routers running BGP, and is easy to be implemented.

There are also many measurement studies on routing attack related problems, for example, analyzing route changes and their causes, measuring how the end-to-end

performance is impacted by protocol policy, and studying black-holes in the Internet [10-13]. Here, we make some control measurement to prevent the potential invalid route attack, to narrow down the scope of the attack. Since the attack is carried on by following the protocols, we identify changes when the attack happens, and record some parameter thresholds, helping better understand the characteristics of the attack.

3 Attack Description

3.1 Methodology

Invalid route injection attack aims at routers running intra-domain protocols. The attackers first establish neighbor relationship with routers in the AS, after that it will advertise many invalid routes to impact the border routers, eventually make other routers in the area affected. Since the border routers are core equipment of the network, it is difficult to attack them directly. Instead of acquiring control of BGP, invalid route injection attack is manipulated by using features of OSPF or IS-IS protocols. It will cause depletion of routers' resource and instability even a loss of connectivity in the network.

To validate the effectiveness of the attack presented above, we design a topology similar to the real network, and simulate the attack on the topology. Since the results of this experiment have nothing to do with the specific autonomous system, the real autonomous system number is not necessary. We use Cisco 1800 series routers in the experiment.

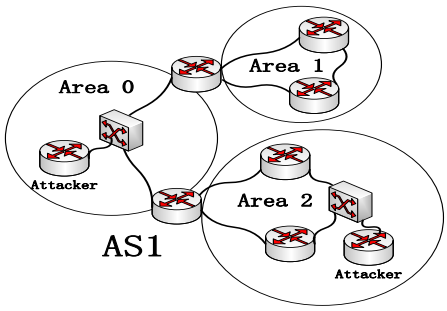

Fig. 1. Invalid Route Injection

The set of intra-domain routers is defined as R_r = {router-id} each element represents a router that is identified by its router-id. $C_{router\text{-}id}$ represents the memory size of each router. The maximum memory within the router can be expressed as:

$$C_{max} = \max \{ C_{router\text{-}id} \}$$

The minimum memory within the router can be expressed as:

$$C_{min} = \min \{ C_{router - id} \}$$

The amount of memory occupied by the attacker's invalid route is defined as Y. Theoretically, $Y \geqslant C_{max}$ means that memory resource of the routers within the entire domain is exhausted after the injection; $C_{min} \leqslant Y \leqslant C_{max}$ means that part of routers' memory resources has been used up; $Y \leqslant C_{min}$ means the injection would not affect the area. Since the router not only handles protocol interactions but also does packet forwarding and calculation of routing paths, the impact of the amount of memory above on a router is an upper bound. Figure1 illustrates the invalid route injection attack, the basic principle of the attack is to add controlled router in the stub by establishing OSPF/IS-IS neighborhood with normal routers, meantime declaring a large number of false or invalid transient messages, thus resulting in many routers' resources deplete in the network. By means of DDoS (Distributed Denial of Service) theory, it will impact the routers of the entire network including high-performance boarder routers through deploying distributed controlled routers.

3.2. Implementation of the attack

1) Attack position.

First we choose a position to attack. Since previous attacks require to know about the core routers or to get the status of the entire network topology in advance, they are difficult to be carried out. However, invalid route injection attack only needs to find routers running OSPF/IS-IS protocol in the stub and to establish OSPF/IS-IS neighbor relationship with normal routers. Hence, it is much easier to implement in practice.

2) Invalid route generation.

Next we generate a lot of static routes as invalid injection. There are many ways to introduce static routes. For instance, we can probe the data layer such as traceroute and ping to get the network segment address, and accordingly to generate a lot of static routes. Also it can be generated in random. After that, the invalid routers can be propagated into the network by flooding mechanism of the protocol, and exhaust the CPU, memory and other resources, thereafter affecting the entire network.

3) Invalid route injection.

Then, we inject route in the network. The way of injection depends on routing protocol running among routers in the network. If using OSPF, the attacker would establish OSPF neighbor relationship with the routers and generate invalid routes redistributed into OSPF, and affect other local routers and other routers in the network; If using IS-IS, the attacker would establish IS-IS neighbor relationship, and directly inject the invalid entries into the IS-IS network.

4) Invalid route revocation.

Finally, in order to advance the attack impact, we revoke or add static route repeatedly to affect the entire network. It will cause the control plane unstable and make the network in a turbulent environment. Thus routers would consume routers' resources, and packets forwarding and neighbor relationship establishment would be affected among routers.

4 Simulation and Experimental Analysis

4.1 Definition of evaluation

In order to demonstrate the effect of invalid route implantation to the network, we define three evaluation indicators for routers: average CPU utilization, average memory utilization and average packet loss rate. Routers' average CPU utilization is calculated as follows:

$$\text{AVE\_CPU} = \frac{\sum_{i=1}^{p}\sum_{j=1}^{q_p} D_{ij}}{M} \tag{1}$$

Let p be the number of the AS, q_p be routers' number in AS p, we define D as CPU utilization, M as total number of routers in the network.

Memory utilization of a router is expressed as:

$$\text{AVE\_Mem} = \frac{\sum_{i=1}^{p}\sum_{j=1}^{q_p} \frac{B_{ij}}{O_{ij}}}{M} \tag{2}$$

As the same, p is the number of the AS, q_p to be router number in AS p, we denote B as memory footprint of a router, O as a router's total amount of memory, M as total number of the routers in the network.

Average packet loss rate is calculated as equation [3]. Here, p represents the number of packets sent, S_i means packets number of the i-th, A means the packets number that have been sent successfully for the i-th.

$$\text{AVE\_Loss} = \frac{\sum_{i=1}^{p} \frac{A_i}{S_i}}{p} \tag{3}$$

4.2. Network topology and experiment design

As shown in Figure 2, AS1, AS2 and AS3 represent different autonomous system; connection among them has been marked. The topology of each AS is shown in Figure 3, there are three areas in one AS, each AS has eight routers, and three routers in area 2 can connect multiple hosts or packet tester.

In the experiment, we first make the network reach a steady state and add attacker in area 2 or area 0 respectively according to the methodology described in Section3. Then we inject a large number of static routes and observe changes in CPU utilization, memory utilization and packet loss rate. Since the value of CPU utilization and memory usage have instantaneous effect, we need to wait for the network to be stable again after the injection and calculate the statistics for router's CPU, memory usage.

We wait about 15 minutes after the injection. The router CPU utilization for each router is calculated using the following formula:

$$B = \frac{\sum_{i=1}^{p} R_i}{p} \tag{4}$$

We denote p as times of calculation, Q measures CPU utilization rate for each time. When checking the router CPU utilization, we type in 'show processes' in the command line of the router. Three values of CPU utilization will be showed, which respectively represent the value within nearest 5 seconds, nearest 1 minute and nearest 5 minutes. In order to ensure the accuracy of the data, we adopt the CPU utilization values within five minutes for each time.

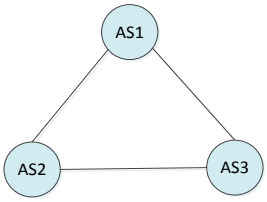

Fig. 2. Topology of Simulation

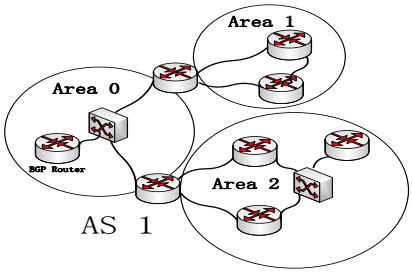

Fig. 3. Topology of AS1

Memory footprint is calculated as equation (5), let p represent times we check, R to be the footprint of each view. We type 'show memory' in the command line to check the memory utilization of the router.

$$D = \frac{\sum_{i=1}^{p} Q_i}{p} \tag{5}$$

4.2 Experimental analysis

Figure 4 reflects changes about the average CPU utilization of the router. In two attackers' situation, with the invalid route entry increasing from 10000 to 80000, the percent of average CPU utilization rise rapidly from 5% to 90%, followed by it is in smooth change. Comparing two attackers' case with the only one attacker situation, the former one has higher average CPU utilization. Also there is a large gap between them, indicating a plurality of attackers would have a greater impact on the network.

Within a certain period of time, the CPU processing capacity of a router is limited. When too many invalid routes injected, CPU utilization is so high that other processes are blocked to take CPU. Thus we draw a conclusion that the attack does have an impact on the packets forwarding and neighborhood establishment.

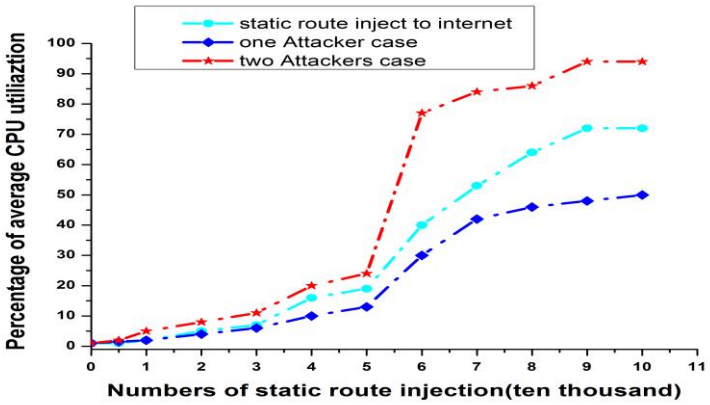

Fig. 4. Average CPU Utilization Trend

Figure5 shows router average memory utilization changes with the number of injected invalid routes. In two attackers' situation, with the increasing of invalid route injection, the average memory utilization strikes a steady upward trend at the initial phase. When injection entry reach 80000, the average memory utilization reaches 90%, and then leveled off. It means that when there are enough static routes, the attack will consume almost all the memory of routers. Then we continue to increase the number of static routers, the utilization increasing is no longer in linear trend but stabilized. Since the router's memory is limited, when the invalid routes occupy too

much memory, it will affect the normal operation of routers, and have an impact on the establishment of neighbor relations and packets forwarding.

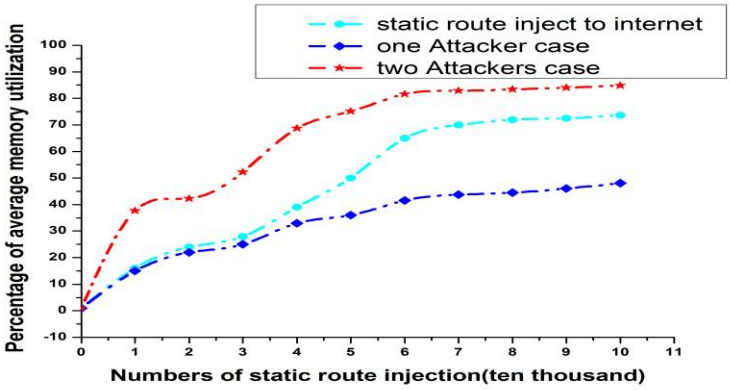

Fig. 5. Router Average Memory Utilization

With the injection of invalid route, packet loss rate throughout the network is shown in Figure 6. In two attackers' situation, the basic network data packets are rarely lost when the invalid route entry is less than 50000, However, the invalid entry and the packet loss rate are increased significantly with the increasing of invalid entry. While the invalid routes reached 60000, packet loss rate is 70%. While 100000 entries, the packet loss rate could even reach 95%. As shown in the figure, the tendency of the network packet loss rate is in line with the average CPU utilization and average memory utilization. The number of Attackers could result in a big gap in the router packet loss rate, before and after the attack, providing that more Attackers, greater impact on the network.

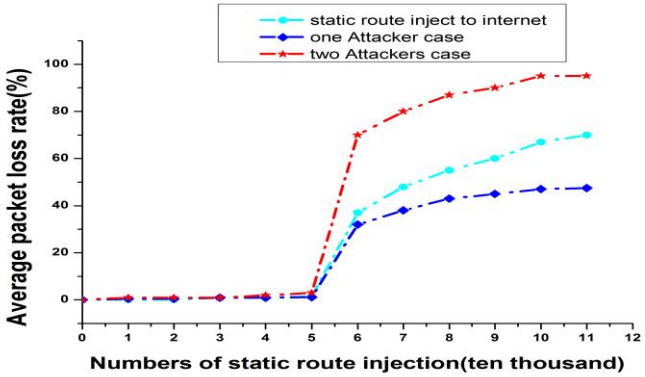

Fig.6. Packet Loss Rate Trend

5 Preventive Measures

5.1 Method for the time introducing route of BGP

According to the attack principle, routers will be affected if an invalid route injects into the network in the corresponding AS. However, if BGP router's reachability information in the corresponding AS is brought into the network through the static mode, the attack will not spread to other AS, thereby narrow down the affected scope of invalid route injection attack.

In Figure 4, within two Attackers in the network, the average CPU utilization of the router changes significantly after we set one static route of into the network. When invalid route entry injected reach 60000, there is 35% gap increase, and the gap will remain at this level following the increasing number of injection. Routers' memory utilization has direct relation with the number of injection. Introducing a router in a static way will influence number of invalid route in the network. It can be seen in Figure 5, at the initial stage, the average memory utilization of the router already has about 20% gap, then gradually stabilized. Similarly, the packet loss rate shown in Fig.6, the difference began to become larger, about 25% when invalid route injection entry reach 60000, in line with the trend of average CPU utilization and average memory utilization.

5.2 Warning threshold for routers

The invalid routes injected to the network could be learned and propagated by routers. We can deploy route entry detection system in service provider's network. Once the route entry detected is beyond a certain baseline, we will make a warning alarm to remind the provider to take measures and reduce losses caused by the attack.

The above methods and other preventive measures such as: the use of QOS mechanism to control the level of security resources [8], modify the route protocol [14-16], with a variety of detection methods [10-13] to check the attacks. Those are not the fundamental solution for static route injection attacks. To prevent attacks fundamentally, we need redesign the existing router or amend the protocols to strengthen network security and prevent attacks against the protocols radically.

6 Conclusion

Through in-depth study of network route protocols, we investigate the invalid route injection attack which can cause severe damage to the network. The key point of the attack is to declare a large number of invalid route information into the network resulting in massive route updates, eventually causing routers' resources exhausted in the network. Meanwhile we provide the specific steps in the generation

and injection of invalid route. We also verify the attack by experiment and analyze the changes in the network after attacks. Finally, we discuss some preventive measures of the attack. These measures can reduce the losses caused by the attack effectively.

7 Acknowledgment

This is supported by Research Foundation of Education Bureau of Hebei Province (No. Z2013124).

8 References

1. Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP)[J]. Selected Areas in Communications, IEEE Journal on, 2000, 18(4): 582-592.
2. Ospf version2, http://www.ietf.org/rfc/rfc-2328.txt
3. Kevin B, Toni F, Patrick M, et al. A survey of BGP security. In: Pro-ceedings of ACM Internet Measurement Workshop, New Orleans, LA,Nov 2005.
4. Murphy S. BGP security vulnerabilities analysis. IETF Internet RFC, RFC 4272, 2006.
5. RIPE, "Youtube hijacking: A ripe ncc ris case study," http://www.ripe.net/news/study-youtube-hijacking.html, 2008.
6. Schuchard M, Aohaisen A, Kune D,et al. Losing Control of the Internet: Using the Data Plane to Attack the Control plane[C]//Proc of the 17th ACM Conf on Computer and Communications Security. New York:ACM,2010:726-728.
7. Bornhauser U, Martini P. About prefix hijacking in the Internet[C]//Local Computer Networks (LCN), 2011 IEEE 36th Conference on. Bonn: IEEE, 2011: 143-146.
8. Liu Y, Su J, Chang R K C. LDC: Detecting BGP Prefix Hijacking by Load Distribution Change[C]//Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International. Shanghai:IEEE, 2012: 1197-1203.
9. Lad M, Massey D, Pei D, et al. PHAS: A prefix hijack alert system[C]//Proc. USENIX Security Symposium. 2006, 2: 153-166.
10. Zheng C, Ji L, Pei D, et al. A light-weight distributed scheme for detecting IP prefix hijacks in real-time[J]. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 277-288.
11. X. Hu and Z. M. Mao. Accurate Real-time Identification of IP Prefix Hijacking[C]// Security and Privacy, 2007. SP'07. IEEE Symposium on. Berkeley, CA:IEEE, 2007: 3-17.
12. White R. Securing BGP through secure origin BGP (soBGP). The Internet Protocol Journal, 2003,6(3):15 − 22.
13. Oorschot P C, Wan T, Kranakis E. On interdomain routing security and pretty secure BGP (psBGP)[J].ACM Transactions on Information and System Security (TISSEC), 2007, 10(3): 11.