IP Prefix Hijacking Detection Using the Collection of AS characteristics

Seong-Cheol Hong[1] and James Won-Ki Hong[2]
[1]Dept. of Computer Science and Engineering
[2]Division of IT Convergence Engineering
POSTECH, Korea
{[1]pluto80, [2]jwkhong}@postech.ac.kr

Hongtaek Ju
Dept. of Computer Engineering
Keimyung University, Korea
juht@kmu.ac.kr

Abstract— **IP prefix hijacking is a well-known security threat that corrupts Internet routing tables and has some common characteristics such as MOAS conflicts and invalid routes in BGP messages. We propose a simple but effective IP prefix hijacking detection method which is based on reachability monitoring. Network reachability means a characteristic that a packet must reach the destination network although the network path is changed due to routing instability. However, when IP prefix hijacking occurs, the traffic sent to victim network does not reach the intended destination but is delivered to attacker network. By identifying the characteristics of the destination network such as network fingerprints, we can know whether the traffic reach the correct destination. In this paper, we present the method of collecting network fingerprints for verifying destination reachability and also propose an IP prefix hijacking detection method using the collected fingerprints. The IP prefix hijacking detection method based on network reachability is effective and useful, which uses a simple active probing and denotes a present network condition.**

Keywords-BGP Security; IP Prefix Hijacking; Fingerprinting

I. INTRODUCTION

The Internet is a decentralized network comprised of many interconnected networks. Each network communicates reachability information using BGP (Border Gateway Protocol). BGP is the de-facto inter-domain routing protocol that maintains a table of Internet Protocol (IP) networks or prefixes, and designates network reachability among the various Autonomous Systems (ASes) that make up the Internet. There are more than 33,000 such systems in the Internet routing system [1]. The routers maintain and update their own routing table according to the routing information exchanged via BGP.

The Internet was designed to provide communication on the basis of trust between networks, but this is been proved to be a wrong assumption, because of various types of attacks. ASes that exchange BGP information directly with each other are assumed to be trusted, so BGP does not implement security checks to protect against receiving invalid routing information from other routers, such as checking the authenticity of origin information and path attributes. As such, the Internet routing infrastructure is vulnerable to attack. IP prefix hijacking is a BGP security attack, in which a BGP router, for malicious purposes or by misconfiguration, announces an IP prefix that the router does not own. This false announcement creates reachability problems and communication failures throughout the Internet. IP prefix hijacking incidents are often reported on the NANOG mailing list [2].

To mitigate the impact of incorrect routing information, some BGP extensions have been proposed, such as Secure BGP (S-BGP) [3] and Secure Origin BGP (soBGP) [4]. These solutions can possibly solve some of the well-known BGP security problems, but they are difficult to deploy in practical networks because the digital signature techniques that are used by S-BGP and soBGP causes high processing overhead, and they are vulnerable to Denial of Service (DoS) attacks. Also, these improved protocols require changes to the existing protocol and infrastructure. So these solutions are not currently deployed, thus other approaches that can detect and respond to IP prefix hijacking are researched.

Many of the previous studies have proposed methods to detect IP prefix hijacking events [5]-[10],[14],[17]. These are easily deployable solutions using passive monitoring or active probing. Some of these approaches, however, use routing registry information, such as IRR (Internet Routing Registry) databases, which can become outdated. The IP prefix hijacking events must be distinguished from legitimate routing updates, because both cases cause Multiple Origin AS (MOAS) changes (i.e. a conflict caused by a particular prefix that appears to originate from different ASes).

A practically deployable, simple and useful IP prefix hijacking detection method is needed in order to respond to increasingly serious IP prefix hijacking incidents. It requires that IP prefix hijacking could be immediately and accurately detected as soon as the hijacking event occurs. Also, it can detect the hijacking incident without constructing an infrastructure which needs mutual cooperation between ASes. An ideal IP prefix hijacking detection method should be easily

This research was supported by the WCU (World Class University) program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. R31-2010-000-10100-0), the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by NIPA (National IT Industry Promotion Agency) (NIPA-2011-C1090-1131-0009) and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0028239).

adoptable and be able to detect all the hijacking attacks regardless of attack types.

We propose a new approach which practically and effectively detects IP prefix hijacking based on network reachability. Network reachability is a decision whether a traffic sent by someone can reach an intended network. In other words, it means that sent packets reach to an original network owning a specific IP prefix, not a destination simply having its prefix. Network reachability defined above should be maintained although the network path is changed due to routing instability. Therefore, the proposed method identifies whether we can reach the previous network through the changed path when a routing update message is arrived and routing path is changed. If we can reach the identical network, the update is regarded as a normal routing event. If not, we decide that it is an IP prefix hijacking.

We use a fingerprinting scheme in order to decide network reachability to a specific network. We classify the type of fingerprints into host fingerprint and network fingerprint. Host fingerprints are the implementation specifications of operating system and protocol stack, or the current configurations of a running application in the host. Network fingerprint is a feature which characterizes a specific network, for example, a value representing host availability in the network. We preliminarily collect the host and network fingerprints of an AS owing a specific IP prefix, then we compare those with currently identified fingerprints of the AS whenever a suspicious routing update is received. In this paper, we propose host fingerprinting and network fingerprinting methods for IP prefix hijacking detection.

One of the most difficult problems for collecting network fingerprints is that it is difficult to collect network information due to firewall or IDS devices. For performing network fingerprinting, we propose a method that preliminarily collects firewall or IDS policies in the target network, and then applies those policies to network fingerprints collection. On the other hand, in host fingerprinting, we should be concerned about how we characterize hosts of the IP prefix. We use Domain Name System (DNS) as the target of host fingerprinting for IP prefix hijacking detection. A DNS server are an appropriate target to collect host fingerprints, and we propose a effective host fingerprinting method of DNS servers for IP prefix hijacking detection.

Although our approach depends on a probing technique for network reachability monitoring, it can conclusively detect an IP prefix hijacking occurrence according to a fingerprint comparison. Also, the proposed method does not depend on monitoring infrastructure such as distributed vantage points in the Internet because an AS receiving routing updates detects IP prefix hijacking for itself. And the work to collect fingerprints is a simple and effective method using popular tools such as ping or traceroute. We validated the effectiveness of the proposed method and are preparing to apply it to the real network.

In this paper, first investigation is made on the IP prefix hijacking problem and provides a classification of IP prefix hijacking scenarios. This comprehensive attack taxonomy provides the foundation for our discussion in this paper of IP prefix hijacking detection. To detect an IP prefix hijacking event, monitor the routing update messages that show an incorrect announcement of their IP prefix origin. When IP prefix hijacking occurs, there must be two networks having the same IP address space in the Internet. Because the basic route selection process is to select routes with the shortest path, only the ASes close to the attacker's AS and are likely to be polluted. We focus on fingerprinting two ASes having the same IP prefix to distinguish IP prefix hijacking events from legitimate routing updates. In this process, live IP addresses are needed for fingerprinting two ASes, so we selected DNS servers for live IP address candidates. Finally, this paper proposes a practical and deployable IP prefix hijacking detection algorithm using DNS servers in the Internet. Our experience of developing the IP prefix hijacking detection system provides a firm guideline for understanding IP prefix hijacking countermeasure mechanisms. Overall, an attempt is made to propose an easily deployable method that performs the detection process without need for AS mutual cooperation or modification to routing protocols and current routers.

The paper is organized into five different section, Section 2 deals with the related work on IP prefix hijacking problem. Section 3 describes a network reachability monitoring. Our proposed solution for IP prefix hijacking direction is presented and explained in section 4 and conclusion and future work in section 5.

II. Background and Related Work

IP prefix hijacking is caused by an attack on the inter-domain routing protocol. The RPSEC (Routing Protocol Security Requirements) working group has released a number of Internet-Drafts regarding a scheme to improve routing protocol security, for example, general security threats and requirements of routing protocols [11, 12]. Path attributes and Network Layer Reachability Information (NLRI) authentication is one of the requirements. This provides a means to verify and assure peer relationships and prefix advertisements against unauthorized announcements. We categorize research on BGP security and IP prefix hijacking detection, to show trends in the development of knowledge in this area.

The Internet is composed of tens of thousands of ASes that are under separate administrative domains. The BGP is the de-facto inter-domain routing protocol. BGP is a path vector protocol in that a BGP update includes a list of ASes which describes the path to a destination address prefix. A destination prefix is usually announced either by the prefix owner itself, if it runs BGP and has an AS number, or by its upstream provider AS(es).

IP prefix hijacking is a well-known security threat, which corrupts Internet routing tables. Because there is no authentication mechanism used in BGP, a malicious or misbehaving 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 IP prefix hijack attacks. IP prefix hijacking is sometimes used by malicious users as a means to illegally obtain IP addresses for spamming or launching Distributed Denial of Service (DDoS) attacks.

Former works in cryptography provides integrity of routing information. One of the BGP security architectures is S-BGP [3], which employs three security mechanisms – Public Key Infrastructure (PKI) for the secure identification of BGP speakers, ASes, and address blocks; Attestations to ensure the authenticity and integrity of data for route and address attestations; and use of the IP security (IPsec) protocol to secure point-to-point communication between BGP speakers. S-BGP requires collaboration with Internet registries and ISPs to set up PKI. However, PKI causes high overhead and requires a wide deployment in the Internet registries, router vendors and ISPs. The other proposal is soBGP [4], which uses certificates dedicated to authenticating AS peers. It then uses two additional certificates (to prove that an AS has the authority to advertise a block of addresses and to certify the advertisement as conformant to a policy of the originator). Even though S-BGP and soBGP are able to solve the security problems of a routing protocol, it is not easy to deploy these solutions in the current Internet infrastructure.

As mentioned above, there are some problems and limitations in cryptography techniques to respond all of IP prefix hijacking cases. So many previous studies have proposed methods to detect IP prefix hijacking events. The IP prefix hijacking detection schemes have some characteristics such as the type of used data, detection subject and attack type. There are control plane and data plane information in the type of used data in order to detect IP prefix hijacking. The control plane is the part of the router architecture, and the detection system uses the information in a routing table or collected with routing protocols. The methods using data plane information rely on active probing in real-time, and then analyze the probing results to know whether an abnormal case occurs. The detection subject is categorized into victim-centric which monitors only its own network, infrastructure-based which uses a centralized database or a set of vantage locations, and third-party which analyzed routing message through own network and detects a suspicious case in the Internet. Finally, in hijacking attack types are prefix hijacking, which contains regular prefix hijacking and sub-prefix hijacking, and AS path falsification which fabricates a path attribute in an update message.

Zhao et al. [13] first explained that the MOAS conflict means that multiple origin ASes announce the same IP prefix. Originally, a unique AS number is allocated to each AS for use in BGP routing. However, the use of static routing and private AS numbers, for example, can cause MOAS conflicts in the Internet [14]. When looking only at BGP update messages we cannot find a difference between legitimate MOAS conflicts, and those caused by IP prefix hijacking.

Lad et al. [6] proposed a method which monitors the occurrence of new origin ASes in real time and notifies the prefix owners that a suspicious update has occurred. However, this method needs to rely on mutual cooperation between ASes. Karlin et al. [15] proposed a system that automatically delays the use and propagation of suspicious routes. Introducing a delay gives the human operators and systems time to investigate the suspicious routes. The routers identify suspicious routes by consulting a table of trusted routing information learned from the recent history of BGP update messages. This method has some false positive cases which can legitimately occur: provider change and occurrence of a previously unseen provider.

Table 1 presents a comparison of the various IP prefix hijacking detection works, including the type of used data, detection subject and attack type. Many works are being researched with different characteristics of IP prefix hijacking detection.

Existing proposals used control plane or data plane information to detect anomalous behavior. The techniques to use control plane information perform analyzing routing table and passive monitoring of BGP routing updates. Such routing information implies an abnormal symptom such as origin AS changes and false AS edges. Data probing schemes provide a way to check reachability to destination prefix at the monitoring moment. It is important to properly select monitors that are able to collect host properties or measure hop count to an IP prefix.

TABLE I. COMPARISON AMONG ANOMALY DETECTION SYSTEMS

Research work	Type of used data		Detection subject			Attack type	
	routing information	data probing	victim-centric	infrastructure-based	third-party	prefix hijacking	AS path falsification
Topology [5]	V			V		V	V
PHAS [6]	V			V		V	
Distance [9]		V		V		V	
Fingerprint [14]	V	V		V	V	V	V
pgBGP [15]	V				V	V	
iSPY [10]		V	V			V	
Strobelight [17]		V	V			V	
Reachability (proposed)	V	V			V	V	V

We classify the detection techniques into victim-centric, infrastructure-based and third-party schemes according to detection subject. Victim-centric detection systems are monitoring potential hijacking of its own prefixes or corporate networks, and the prefix owner makes hijacking detection decision locally. There are two types of infrastructure-based approaches. One uses a centralized database such as RouteViews and RIPE RRC which collect real-time information about the global routing system from several different backbones and locations around the Internet. The other uses a set of vantage points in order to collect several of active probing results and compare those with the past data or each other for detecting IP prefix hijacking. The detection systems using third-party schemes analyze routing message through own network and apply the detection algorithm with the message in order to identify whether a suspicious event.

The attack types of IP prefix hijacking divide into prefix hijacking and AS path falsification. Prefix hijacking means that an attacker makes an IP prefix hijacking by falsifying the NLRI field of a BGP update message. Regular prefix hijacking and sub-prefix hijacking clearly have different influences from the polluted and unpolluted ASes point of view. However, we do not need to deal with regular prefix hijacking and sub-prefix hijacking separately in our approach. AS path falsification attack occurs when an attacker modifies a path attribute of update message for IP prefix hijacking.

Compared to other approaches, our proposed method uses both routing information and data probing, covers all attack types of IP prefix hijacking and focuses on the third-party scheme. The existing proposals using one of the two types of used data have some limitations such as not covering all attack types. The approaches using both control and data plane information can increase the detection accuracy. Also, the proposed method uses the third-party scheme in order to detect the hijacking incident without constructing an infrastructure. Therefore, our proposed method can be easily adoptable and detect all of the hijacking attacks regardless of attack types without mutual cooperation between ASes.

III. Reachability Monitoring

The Internet is a huge and decentralized network comprised of ASes which exchange routing information using BGP. The goal of routing is selecting a path which can send network traffic between not directly connected hosts. However, network communication is affected by the changes of routing path, network topology and device configuration.

Network reachability is a decision about whether a traffic sent by someone can reach an intended network through a path announced by routing protocol. The network reachability cannot be guaranteed by BGP routing because of a physical failure or a software error at network devices. In other words, we cannot be sure of the network reachability to destination just by knowing only routing information. Therefore, we need to identify the network reachability by performing an actual verification such as active probing.

IP prefix hijacking is an attack which influences the network reachability. When IP prefix hijacking occurs, network traffic is delivered to the attacker network, not the destination network. That is, network reachability to the destination network is not guaranteed. If we know preliminary information about the destination network and analyze responses by active probing based on that information, then we can identify whether the network reachability is guaranteed. In this paper, we propose an IP prefix hijacking detection method using the approach mentioned above.

When we monitor network reachability, it is a difficult problem to determine how to collect characteristics about a specific network. Network reachability monitoring usually depends on active monitoring techniques because there is a bit limitation to data collected by passive monitoring and it is difficult to analyze the data in real-time. Existing reachability monitoring among active monitoring techniques uses a direct method using ICMP which is used in tools such as *ping* or *traceroute*. However, ICMP packets are suffered from improved network security policies when they pass through a firewall or the Internet junction in an enterprise network. Also, an end-host can filter ICMP packets or not respond to active probing packets. We must make an appropriate probing packet and select a host which always responds to it in order to collect network characteristics through a firewall. In other words, a combined method should be applied because there is limitation to data collected by using existing tools.

In this paper, we perform the collection of network characteristics with two approaches. One is to perform host fingerprinting by selecting some hosts which are representative servers in the target network, for examples, web or DNS servers. A probing packet to the services provided on these servers can easily pass through a firewall and the servers should properly respond to a received packet. Therefore, without the deep regard to network security we can collect host fingerprint information about a host running as a server at any time. The other is to perform network fingerprinting by inferring a network firewall policy and using it as a network characteristic. We design an effective method to accurately infer a firewall policy by performing active probing to a target network.

IV. IP Prefix Hijacking Detection Method

Our motivation is based on the fact that, existing BGP security solutions are not applicable to deal with all IP prefix hijacking cases. Filtering is used mostly to defend against invalid updates announced by 'stub ASes', but it cannot cover 'transit ASes.' And it is impractical to deploy cryptographic techniques to all the routing devices in the Internet. Also, traditional probing methods cannot detect IP prefix hijacking effectively due to enhanced Internet security. So a novel approach is need which can cover all IP prefix hijacking threats.

In this section, an attempt is made to propose a novel IP prefix hijacking detection method which can be applied in the current Internet environment. Two important approaches as follows:

1) Develop a better probing method by responding more to the probing packets in hosts for reachability monitoring.

2) Develop a practical IP prefix hijacking detection algorithm based on BGP threat analysis.

This section explains how to collect live hosts for host fingerprinting and how to infer firewall policies in the network for network fingerprinting. Fingerprinting methods are presented and followed by proposed detection algorithm.

```
Input: BGP routing tables (RIB)
Output: Live IP set and AS fingerprint

Phase 1: Collect live IP set composed of (IP prefix, Internet Servers)
IP_PREFIX = all IP prefixes from RIB
For each ip_prefix in IP_PREFIX
    dn = authority resulted from DNS reverse lookup with ip_prefix
    if dn exists
        MX_ip = DNS MX query with dn
        web_ip = inferred from dn
        live_ip[ip_prefix] = (DNS_ip, MX_ip, web_ip)
        as = AS containing ip_prefix
        ip_list[as] = ip_list[as] U live_ip[ip_prefix]
    else
        live_ip[ip_prefix] = null

Phase 2: Collect AS fingerprints
ASes = all ASes appeared in RIB
For each as in ASes
    type[as] = determine transit or stub AS
    degree[as] = compute the connection degree
    rtt[as] = measure RTT from monitoring system to ip_list[as]
    geo[as] = geographical distance from monitoring system
```

Figure 1. Pseudo-code for the collection algorithm

A. *Host fingerprinting*

To detect IP prefix hijacking, we need a reachability test for all ASes by active probing. ‘Reachability’ means determining whether data can be delivered along a configured path by routing. The current routing table does not guarantee the reachability of all destination ASes, so we need to confirm the reachability by real-time testing to detect IP prefix hijacking.

Live host constraints for reachability monitoring are as follows: 1) operated in most of ASes, 2) easy to obtain IP addresses, 3) always provide services for its AS, and 4) allow external connection and respond to active probing. We use a DNS server as live hosts because it is a core infrastructure in the Internet which always provide services and allow external connection from any hosts.

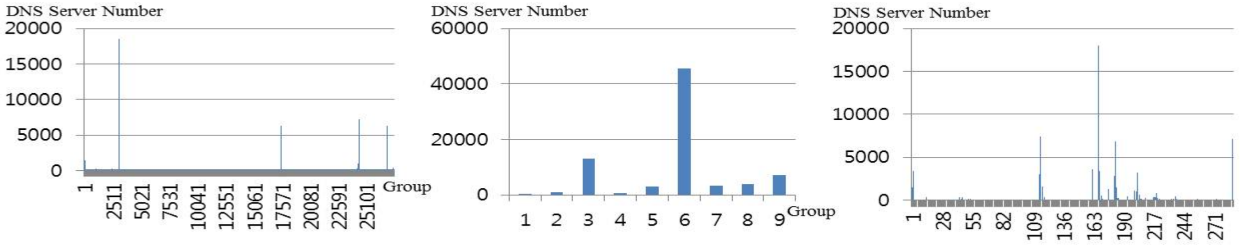
First, build a current Routing Information Base (RIB) based on the information obtained from RouteViews [16]. RIB consists of IP prefixes (IP_PREFIX) and the routing path to its (AS_PATH). To collect a live host for all IP prefixes, we use reverse DNS lookup querying to local DNS and global DNS servers. Reverse DNS lookup is a query returning domain names for an IP address. The first query is to get an authority server having the authority for a particular IP prefix. The second query is to obtain an IP address through querying with the domain name of a DNS server. If we fail to get information from a local DNS server, we use a global DNS server. And if we get the domain name of a DNS server, will infer a mail server or web server using the domain name's part.

Next, we are adding a DNS server’s address to ‘AS.set’ which is a DNS server address set obtained from the phase 1 process. If AS.set is equal to AS.rib.origin, we conclude that there is a DNS server in the AS which is obtained from RouteViews. If AS.set is different from AS.rib.origin, AS.Set.Count is incremented and it is used to know DNS server’s operation status for the IP prefix. We separately construct DNS server lists for DNS servers operated both inside and outside AS, then the lists will be used to decide the validation of active probing. Also, we send a DNS query to the server and store the response to know its service status.

Then, we perform the process that collects the preliminary information and decides MOAS occurrence. We collect several data for applying the proposed detection method: current routing table information (destination IP prefix and as path), DNS server information (DNS IP address per AS and host fingerprint), network fingerprint (internet server’s IP addresses and Round Trip Time (RTT) to AS), and threshold values (geographically allowed distance and RTT between two neighbor ASes). Then we extract IP prefix and as path from a BGP update message and analyze it using preliminarily collected information.

The DNS server list is collected from RouteViews Prefix over the three months, from May 2010 to July 2010. We collected preliminary results about distribution of DNS servers in the Internet. We are using the collected DNS server list for performing host fingerprinting by DNS query and reply. The results of host Fingerprinting are obtained, such as DNS software type and version, state of TCP 53 port, uptime of device. The results by DNS query and reply are the authority section and additional section of DNS message, such as aa flag bit status, whether a DNSSEC is applied. And the results are stored in the DNS server fingerprint DB.

We collected the fingerprint information of 77,530 DNS servers and analyzed them which are divided into three categories in order to distinguish each DNS server. The three kinds of categories are DNS protocol, DNS query and DNS host fingerprint. The DNS protocol contains DNS software type and version, uptime. The DNS query contains Authority



a. DNS Protocol

b. DNS Query

c. DNS Host Fingerprint

Figure 2. The number of distinguishable groups in the DNS server fingerprints

TABLE II. The Internet firewall policy of a sample network

Rule	Protocol	Src IP	Src Port	Dst IP	Dst Port	Action
R1	ICMP	Any	Any	192.168.10.*	-	Permit
R2	TCP	Any	Any	192.168.10.*	22-23	Permit
R3	TCP	Any	Any	192.168.10.*	53-80	Permit
R4	UDP	Any	Any	192.168.10.*	1-1023	Permit
Default	Any	Any	Any	Any	Any	Deny

Section, Additional Section and aa bit. And The DNS host fingerprint contains the application of DNSSEC and state of TCP port 53. The x-axis in Fig. 2 is the number of groups and y-axis represents the number of DNS server that belongs to the group. All the DNS servers cannot be exactly distinguished, but we can apply that level of distinction to our proposed IP prefix hijacking detection method.

B. Network fingerprinting

We use the firewall policy of a target network as a network fingerprint. The Internet firewall is deployed at an external point in the network. Inferring the firewall policy should need to be separated the policies of the Internet firewall and host firewall. It is possible to infer host firewall policy if the host is alive. One of several reasons to make the firewall policy's inference difficult is that we cannot suppose that the host is always alive. Therefore, we should infer each of the firewall policies. To infer the Internet firewall policy, probing packets are generated with TTL values assigned the length of path to firewall plus one, and are sent them to destination address. If probing packets are not filtered by the firewall, we can receive the ICMP Time Exceed message. If probing packets are filtered, we cannot receive any response packets. But some firewalls filter out ICMP packets to the Internet. In this case, it is impossible to infer the separate policy for Internet firewall and host firewall. A sample of the inferred firewall policy is described in table II.

C. IP prefix hijacking detection method

When IP prefix hijacking occurs, the BGP speakers subsequently propagate a false announcement by selecting the shortest path as the best path. As the false announcement is propagated, the Internet becomes polluted. Polluted ASes cannot reach the victim network due to corrupted routing tables in the Internet. However, not all suspicious updates are IP prefix hijacking events. So we should distinguish legitimate cases from IP prefix hijacking.

Fig. 3 presents the IP prefix hijacking detection process. As mentioned above, data will be collect for applying the proposed detection method: current routing table information (destination IP prefix and as path), DNS server information (DNS IP address per AS and host fingerprint), network fingerprint (internet server's IP addresses and Round Trip Time (RTT) to AS), and threshold values (geographically allowed distance and RTT between two neighbor ASes). Then we extract IP prefix and as path from a BGP update message and analyze it using preliminarily collected information.

If MOAS occurs, it determines the possibility of host fingerprinting through the existence of DNS servers in the AS. If there is a DNS server in the AS, the detection system sends a User datagram protocol (UDP) or Transmission control protocol (TCP) Domain name service (DNS) query to the DNS server. If the detection system receives a response, it performs host fingerprinting.

If MOAS does not occur, all the links in AS_PATH are validated by the detection system. We calculate the occurrence frequency of each link based on routing table information. If the link is already occurred in the routing table, we conclude that the update message is valid. The newly occurred link is validated by the detection system with geographical distance and RTT from the monitor to each AS of a suspicious link. If distance or RTT gap is significant, we perform the fingerprinting process.

The fingerprinting process performs network fingerprinting when there is not a DNS server inside a target AS appeared in a suspicious update message. The network fingerprinting process infers the current firewall policy by active probing, and then compares the preliminarily collected data. If fingerprints are not matched, we conclude that the update message is generated by an IP prefix hijacking event.

D. System Architecture

Fig. 4 shows an overview of detection system in deployment. The detection system connects to the BGP router in an observer AS to monitor the routing table and BGP update messages. A BGP update message consists of withdrawn routes, the reachability information in the NLRI field and the AS_PATH attribute. The NLRI field indicates the IP address space of the destination AS, and the AS_PATH attribute has the AS level path to reach the announced address space.

```
Input: BGP update message m
Output: decision of valid or invalid update
m has NLRI, origin AS (oAS) and AS_PATH information
we already collected a DNS server and fingerprints from oAS

if m causes MOAS
  if DNS belongs to NLRI
    send a query to DNS
    if response is returned
      compare host fingerprint
      if host fingerprint agreed
        valid update
      else
        invalid update
    else
      compare network fingerprint
  else
    perform network fingerprint
else
  if AS_PATH contains new link
    perform network fingerprint
```

Figure 3. Overall detection algorithm

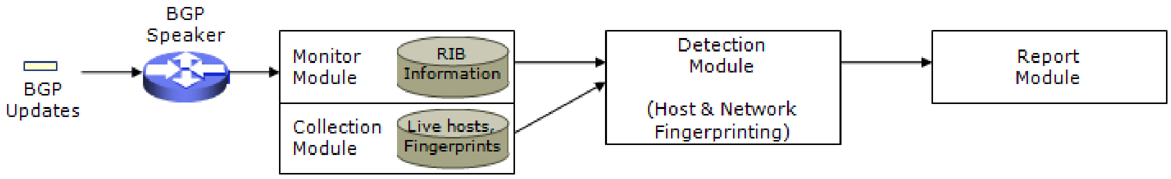


Figure 4. Detection system architecture

By comparing update messages and the routing table, we can observe a suspicious event, especially a MOAS conflict. When a suspicious BGP update such as a MOAS conflict is received, the system starts a detection process to distinguish an IP prefix hijacking event from a legitimate routing update. Because the detection system performs active probing by itself and the router uses existing BGP, it does not need to modify the router's software or routing protocol. Therefore, the proposed method is a deployable approach that uses existing Internet infrastructure.

V. CONCLUSION

Internet routing infrastructure is vulnerable to attack. IP prefix hijacking is a BGP security attack, in which a BGP router, for malicious purposes or by misconfiguration, announces an IP prefix that the router does not own. This false announcement creates reachability problems and communication failures throughout the Internet. This paper reviewed existing works to secure BGP routing, especially IP prefix hijacking detection techniques. Because BGP extensions such as cryptography and PKI are difficult to deploy in practical networks, recent works have researched anomaly detection approaches which analyze routing information and perform data-plane testing. We have proposed a reachability monitoring scheme which can locally detect IP prefix hijacking within an own network. In particular, we have presented the comparison among anomaly detection systems for IP prefix hijacking problem according to different characteristics. Our proposed scheme can provide accurate and deployable properties for applying in the Internet.

To analyze the performance and feasibility of our approach by collecting host and network fingerprinting in the Internet are planned for future enhancement. We also plan to implement a hijacking detection system based on our proposed scheme and apply it to the real research network.

REFERENCES

[1] BGP Routing Table Analysis Reports, "BGP Reports," http://bgp.potaroo.net/.

[2] North America Network Operator's Group, "NANOG: NANOG Mailing Lists," http://www.nanog.org/mailinglist/.

[3] C. Lynn, J. Mikkelson, and K. Seo, "Secure BGP (S-BGP)," IETF Draft: draft-clynn-s-bgp-protocol-01.txt, June 2003.

[4] Brian Weis, "Secure Origin BGP (soBGP) Certificates," IETF Draft: draft-weis-sobgp-certificates-02.txt., July, 2004.

[5] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, "Topology-based Detection of Anomalous BGP Messages," In Proceedings of the 6th Symposium on Recent Advances in Intrusion Detection (RAID), LNCS 2820, Pittsburgh, PA, USA, September 2003, pp. 17-35.

[6] M. Lad, D. Massey and D. Pei, "PHAS: A Prefix Hijacking Alert System," In Proceedings of the 15th USENIX Security Symposium, Vancouver, B.C., Canada, August 2006, pp. 153-166.

[7] M. Tahara, N. Tateishi, T. Oimatsu, S. Majima, "A Method to Detect Prefix Hijacking by Using Ping Tests," In Proceedings of the 11th Asia-Pacific Symposium on Network Operations and Management (APNOMS 2008), LNCS 5297, Beijing, China, October 2008, pp. 390-398.

[8] Z. M. Mao, J. Rexford, J. Wang, and R. H. Katz, "Towards an Accurate AS-level Traceroute Tool," In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Karlsruhe, Germany, August 2003, pp. 365-378.

[9] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, "A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-time," ACM SIGCOMM Computer Communication Review, Vol37, Issue4, October 2007.

[10] Z. Zhang, Y. Zhang, Y. C. Hu, Z. M. Mao, and R. Bush, "iSPY: Detecting IP Prefix Hijacking on My Own," In Proceedings of the ACM SIGCOMM 2008 conference on Data Communication, Seattle, USA, 2008, pp. 327-338.

[11] A. Barbir, S. Murphy, and Y. Yang, "Generic Threats to Routing Protocols," IETF Draft: draft-ietf-rpsec-routing-threats-07, October 2006.

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

[13] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "An Analysis of BGP Multiple Origin AS (MOAS) Conflicts," In Proceedings of the 1st ACM SIGCOMM workshop on Internet Measurement, San Francisco, USA, November 2001, pp. 31-35.

[14] X. Hu and Z. M. Mao, "Accurate Real-time Identification of IP Prefix Hijacking," In Proceedings of the IEEE Security and Privacy, Oakland, California, USA, May 2007, pp. 3-17.

[15] J. Karlin, S. Forrest and J. Rexford, "Pretty Good BGP: Improving BGP by Cautiously Adopting Routes," In Proceedings of the 14th IEEE International Conference on Network Protocols, Santa Barbara, California, USA, November 2006, pp. 290-299.

[16] Oregon Route Views Project, "Route Views Project Page," http://www.routeviews.org/.

[17] James W. Mickens, John R. Douceur, William J. Bolosky and Brain D. Noble. "StrobeLight: Lightweight Availability Mapping and Anomaly Detection."USENIX'09 Proceedings of the 2009 conference on USENIX Annual technical conference, CA, USA, 2009.

[18] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel and A. Rubin, "Working around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing," in Proc. ISOC NDSS'03, San Diego, CA, Feb. 2003, pp. 75-85.

[19] T. Bates, E. Gerich, L. Joncheray, J. M. Jouanigot, D. Karrenberg, M. Terpstra and J. Yu, "Representation of IP Routing Policies in a Routing Registry," RFC 1786, Mar. 1995.

[20] T. Bates, P. Smith and G. Huston, "CIDR Report for 1 Feb 11," http://www.cidr-report.org/as2.0/, Feb. 2011.

[21] Lakshminarayanan Subramanian, Volker Roth, Ion Stoica, Scott Shenker and Randy H. Katz, "Listen and Whisper: Security Mechanisms for BGP", In Proc. Symposium on Networked Systems Design and Implementation (NSDI'04), San Francisco, CA, March 2004