A CGA Based IP Source Address Authentication Method in IPv6 Access Network

Guang Yao and Jun Bi
Network Research Center
Tsinghua University
Beijing 100084, China
yaog@netarchlab.tsinghua.edu.cn, junbi@tsinghua.edu.cn

***Abstract*—In this paper, we present a novel source address spoofing prevention method for IPv6 access network called CGA based Source Address Authentication (CSAA). It makes use of CGA (Cryptographically Generated Address) to generate an unspoofable identifier of host without PKI, and bind it to the authorized address of the host. Then all the packets sent out by the host can be validated in the first-hop router by a light-weight method.**

Keywords-CGA; Source Address Spoofing; IPv6 Access Network

I. INTRODUCTION

IP spoofing is still a pressing problem. Attackers can launch varied attacks by utilizing deliberately or randomly forged addresses. According to the study of CAIDA, there are at least 400 spoofing attacks every day in the Internet [1]. The reason for its popularity is that it is easy to launch an attack and hard to trace the attacker.

There are many mechanisms to prevent IP spoofing. Generally, they are divided into three classes: filtering on path, end-to-end authentication, and traceback. Filtering in access network is a special kind belonging to "filtering on path". This kind of methods focuses on filtering out spoofing packets coming from local access network. Filtering in access network is the best way to block the spoofing packets from harming the Internet. There have been some filtering mechanisms for access network. Ingress filtering [2] is the most famous one among them, but ingress filtering only filters spoofing packets at a very coarse level. Most of the filtering mechanisms with fine granularity rely on binding addresses to a switch port. However, if there is no switch between the host and the router, such methods will be disabled. Moreover, there isn't any mechanism that can suit all the address allocation methods.

CGA [3] is a way to generate IPv6 address which cannot be spoofed by other nodes in the local link. In CGA, the interface ID is generated by hashing a public key, which is generated by the host but not allocated by the PKI. Whenever CGA is used in a packet, the public key and a signature of the whole packet is also contained in the packet. The receiver of the packet can check the correctness of the association of public key and address, and the signature to check whether the address is credible. The verification of CGA address is expensive and it cannot be used in other address assignment mechanisms. Generally, CGA is only used in SEND [4] to secure the ND protocol.

This article proposes a novel method which uses the feature of CGA address, called CGA based Source Address Authentication (CSAA). We use CGA as an unspoofable identifier of the host instead of an address. CSAA can work along with all the address allocation methods and is independent of physical medium. CSAA uses a light-weight method to authenticate the address. Compared with IPSec, CSAA is independent of PKI to authenticate the source address and can adapt all address allocation mechanisms.

II. PROBLEM STATEMENT

The requirements for filtering spoofing packets in IPv4 and IPv6 are different. Considering the features of IPv6, a proper IPv6 access network filtering mechanism should meet the following requirements:

- Support all IPv6 address assignment methods: stateless, DHCP, manually, etc.
- Allow a host to have more than one interface, and allow an interface to have multiple addresses.

III. MECHANISM DESIGN OVERVIEW

CGA based Source Address Authentication (CSAA) is a two-stage method. In the first stage, the host must request the right of using an address from the first-hop router and the router will check the availability of the address. And then, the host and the router exchange a bit string which we call "signature-seed". In the second stage, packets sent out by host must carry a signature which is generated using the "signature seed" and the router checks and removes the signature. Fig 1 shows the procedure of the mechanism.

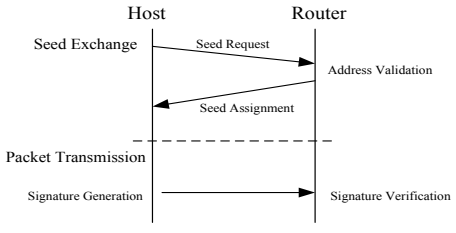

Fig 1. Overview of CSAA

A. Seed Exchange

1) Seed Request: The host first sends a request packet to the first-hop router. This packet is named as Seed Solicit (SS) packet. It is an ICMP packet. The source address of this packet is set to be the address which the host wants to use in the future communication, and the destination address is the address of the first-hop router. This packet contains a Nonce field and a CGA Identifier field. The Nonce field contains a random number to prevent replay attack. The CGA Identifier field is actually the CGA address generated from the public key contained in the CGA Option. The link layer address should be used as a parameter to generate an address. A CGA Option field and a RSA Signature field are also contained in the packet to verify the CGA identifier.

2) Address Validation: Once the router receives an SS packet, the validity of the RSA signature and the CGA identifier is checked. Then it will check whether the source address of the packet is allowed to be used by the host. Apparently, the judgment depends on the address allocation method. The judgment process is described as follows:

- DHCP: Host can only use its CGA address as the source address to send DHCP-SOLICIT to the DHCP server. The router tracks the DHCP-ADVERTISEMENT and find which address is allowed to be used by the host. The CGA address is used as the CGA Identifier in the SS packet. Only SS packets containing the allocated address and the correct CGA Identifier are valid.
- Stateless Auto Configuration: The router will keep a table which maps CGA Identifier to address and records every success Seed Solicitation. The address is allowed to use if no other host is using that address.
- Manual Allocation: The host must fill the Reserved filed with the user name encrypted by the nonce and the public key of the router. The router will check whether the address is allocated to the user.

3) Seed Assignment: After the SS packet is verified, the router will generate a signature-seed by a random number generator. The signature-seed is bound to the source address of applicant. The public key, the CGA identifier, and the nonce value of the applicant can be also bound with the address. Then the signature-seed is encrypted by the public key in the CGA Option of the SS packet. After that, the router returns a Seed Advertisement (SA) packet to the applicant. This packet has the same format as the packet SS, except that the Reserved field is replaced by the Encrypted Seed.

Once the host receives the SA packet, it will check whether the packet is from the router by checking the CGA Identifier field. To ensure that the host knows the CGA identifier of the first-hop router, the router must broadcast its CGA identifier periodically in the Router Advertisement message. Then the host decrypts the Encrypted Seed field to get the signature-seed.

B. Packet Transmission

After the seed exchange, there is some shared secret between the host and the router. The router has a table, named Address Record Table, to record the secret. The entry of this table is as follows:
<CGA Identifier, Public Key, Nonce, Address, Signature Seed>.

We suggest two methods to generate the signature in packet transmission: HMAC, Pseudo Random Number.

These two methods are light-weighted and provide adequate security. The latter is much faster for it doesn't compute using the packet and the signature can be generated in advance. However, Pseudo Random Number must solve the problem of out-of-order sequence, though it seldom happens on the local link.

Whichever signature generation method is chosen, the packet must contain the signature in an IPv6 option header. We suggest choosing the hop-by-hop option header, and the option should be a new type. The router checks the header and removes the header after verification. If the signature is wrong or no signature exists, the packet should be dropped.

IV. Experiment and Performance Evaluation

We have implemented a simple prototype of CSAA and test it in manual allocation and stateless cases, and it works correctly in these situations. The DHCP case is more complex and we plan to implement CSAA in DHCP in the future work.

According to our experience in [5], the speed of signature based authentication can be close to the line speed of a 100Mbps Ethernet. The authentication algorithm can be improved, or implemented in hardware to support higher speed network.

References

[1] CAIDA, http://www.caida.org/data/realtime/telescope/.

[2] P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," RFC 2827, May 2000.

[3] Tuomas Aura, "Cryptographically Generated Address(CGA)," Infomation Security Conference, 2003.

[4] J. Arkko, J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC3971, March 2005.

[5] Guang Yao, Jun Bi, "Design and Implementation of an IPv6 Source Address Validation Device," ICNS, 2008.