Network Working Group H.Rafiee
INTERNET-DRAFT D. Zhang
Updates RFC 3972 (if approved) Huawei Technologies
Intended Status: Standards Track
Expires: February 11, 2015 August 11, 2014

CGA Security Improvement
<draft-rafiee-rfc3972-bis-00.txt>

Abstract

This document addresses the security problems existing in the current CGA specification. It also explain the changes that is needed to take into consideration when the prefix length needs to be variable.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 11, 2015.

Table of Contents

1. Introduction

In the Cryptographically Generated Addresses (CGA) specification [RFC3972], the 64 rightmost bits of an IPv6 address is securely generated with a public key. This solution is able to provides the proof of IP address ownership and then prevent source IP spoofing by finding a binding between the public key and the node's IP address. Unfortunately, during the verification step as explained in [cga-attack], the verifier nodes ignore the 3 bits sec value in the interface ID (IID) and there is no check between the source and target IP address. This problem lead to the case where an attacker can calculate a new CGA address which is identical to the address of the victim node except its sec value field is zero. This document tries to explain how to address this problem.

This document also tries to explain how CGA specification needs to be changed when it is expected to support variable prefix.

2. Sec Value Solution

Sec value in CGA algorithm is the value between 0 to 7. This value shows the strengthen of the algorithm against brute-force attacks. As higher this value is, the more expensive and complicated the algorithm is for the attacker.

As explained in [cga-attack], since there is no check between the source and target addresses and the node ignores 3 bits sec values during verification process, an attacker can try to perform brute-force attacks without being detected. In other words, it does not matter what sec value the legitimate node uses, the attacker can always generate a new CGA address identical to the address of the victim except of the sec value field, and use the address to impersonate the legal node without being detected. To address this problem, we propose the changes in the following section of RFC 3972:

- Section 5. new step MUST be placed before step 1 of verification.

1- If the sender's source address is not a multicast IP address, then the verifier node MUST compare the sender's source address with its own local and global IP addresses. If there is a match it starts the other verification steps. Otherwise, it discards the message silently.

If the sender's source address is a multicast IP address but the target address is a unicast IP address, then the verifier node MUST

compare the target address with its own local and global IP addresses. If there is a match then it MUST process the other verification steps. If there is no match, it should discard the

message silently.

3. CGA and Challenges in Variable Length Prefix

CGA algorithm, by default, uses a 64-bit prefix. The output of this algorithm is a 64-bit IID. This value is the result of hashing function on CGA parameters and taking only 64 bits of the hashing result (digest). To conform CGA with a dynamic prefix length, the number of bits which are taken from the hashing value should be the same size Having a dynamic prefix, as explained in [cga-attack], might lead to the case where the attacker claim the address ownership of other legitimate nodes with different prefix values. This is specially true and feasible when prefixes are longer than 64 bits. In other words, less bits are available for Interface ID.

4. Security Considerations

There is no security consideration

5. IANA Considerations

There is no IANA consideration

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)," RFC 3972, March 2005.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC7136] Carpenter, B., Jiang, S., "Significance of IPv6 Interface Identifiers", RFC 7136, February 2014.

[cga-attack] Rafiee, H., Meinel, C.,"Possible Attack on Cryptographically Generated Addresses (CGA)", http://tools.ietf.org/html/draft-rafiee-6man-cga-attack , Augst 2014

[variableprefix] Carpenter, B., Chown, T, Gont, F.,
Jiang, S., Petrescu, A., Yourtchenko, A.," Analysis

of the 64-bit Boundary in IPv6 Addressing",
http://tools.ietf.org/html/draft-ietf-6man-why64 ,
April 2014

Authors' Addresses

Hosnieh Rafiee
HUAWEI TECHNOLOGIES Duesseldorf GmbH
Riesstrasse 25, 80992,
Munich, Germany
Phone: +49 (0)162 204 74 58
Email: hosnieh.rafiee@huawei.com

Dacheng Zhang
HUAWEI TECHNOLOGIES
Q14 huawei campus, Beiqing Rd., Haidian Dist.,
Beijing, China
E-mail: zhangdacheng@huawei.com