Study of IPv6 Security Issues in Large-Scale Data Center

Sangwook Bae, Heejun Yoon, and Byungyun Kong

Abstract— With the ongoing depletion of IPv4 addresses, large-scale data center are experiencing difficulties to acquire the necessary IPv4 addresses. Therefore, several large-scale data center are actively applying the IPv6(Internet Protocol version 6). IPv6 has an unlimited number of address spaces, and there is an important feature, in that the server can generate and configure its own IPv6 address. This feature is called Stateless Address Auto Configuration(SLAAC). However, this feature has drawbacks related to security in the large-scale data center system. Because a malicious server can make paralyzed or confused to the large-scale data center systems. In this paper, we will discuss what IPv6 security issues in large-scale data center.

Research Keywords— IPv6, Security, Large-Scale Data Center.

1 INTRODUCTION

Currently, several large-scale data centers actively adopt Internet Protocol version 6 (IPv6)[1][2]. IPv6 was developed by the Internet Engineering Task Force (IETF) [3] in 1998 to overcome the limitations of IPv4 [4]. In addition to having a larger address space, IPv6 has additional advantages over IPv4 such as Stateless Address Autoconfiguration (SLAAC) [5], mobility, Quality of Service (QoS), and improved security. In particular, SLAAC procedure allows the server to generate its own address using Internet Control Message Protocol version 6 (ICMPv6) [6] if the administrator connects to the network without preference. However, if a malicious server causes the system to become paralyzed or confused, we should block it.

The remainder of this paper is organized as the follows: Section 2 explores IPv6 security issue in large-scale data center; Chapter 3 concludes the paper and future works.

2 STUDY OF IPV6 SECURITY ISSUE IN LARGE-SCALE DATA CENTER

In this section, we will introduce IPv6 security issues in large-scale data center. We are going to explain 2 kinds of IPv6 security issues. One is modulated neighbor cache tables issue and the other is DAD procedure issue.

2.1 Study 1

This study is IPv6 security issue using modulated neighbor cache table in Large-Scale Data Center.

Normally, each server should create neighbor cache table for communication to others. In this, there are IP address and MAC address for other server like table 1(state2)[6]. It is possible to makes paralyzed and confused to large-scale data center systems using neighbor cache tables like Fig1.

① The Central Manager sends the solicited multicast NS message as a link and performs an address check to verify the MAC address of the execute server3 as shown in Table 1(state1).

② The malicious server intercepts the solicited NS message and then extracts the packet to obtain information from the Central Manager. And execute server3 should sending NA message for neighbor cache update of central manager.

③ The malicious server sends fake NA message to central manager. After that, neighbor cache tables of central manager updates malicious server's MAC as shown in Table 1 (state3).

④ The malicious server sends fake NA message to execute server3. And then, neighbor cache tables

- *Sangwook Bae is with the Korea Institute of Science and Technology Information, Daejeon, South Korea. E-mail: wookie@ kisti.re.kr.*
- *Heejun Yoon is with the Korea Institute of Science and Technology Information, Daejeon, South Korea. E-mail: k2@ kisti.re.kr.*
- *Byungyun Kong (corresponding author) is Korea Institute of Science and Technology Information, Daejeon, South Korea. E-mail:kong91@ kisti.re.kr.*

of execute server3 updates malicious server's MAC as shown in Table 1 (state3).

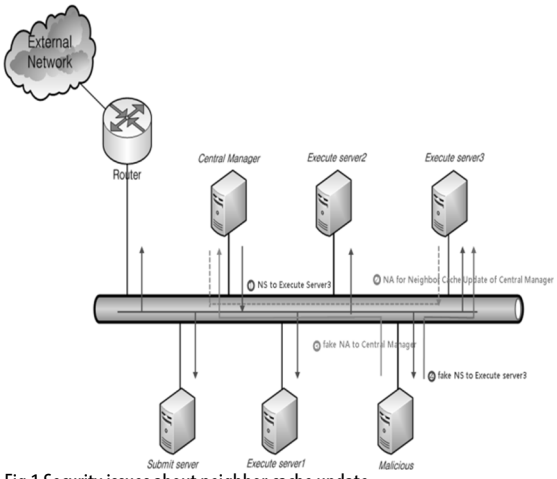

Fig 1 Security issues about neighbor cache update

For a normal neighbor cache update, the neighbor cache status is the same as for table1(state2), but the neighbor cache update is changed to the malicious server's MAC due to an abnormal neighbor cache update on the malicious server as shown in Table 1 (state3).

Table 1 . Neighbor Cache States

State1			
CM(Central Manager)		ES(Execute Server3)	
ES_Link_IP	-	CM_Link_IP	-
ES_Global_IP	-	CM_Global_IP	-
State2			
ES_Link_IP	ES_MAC	CM_Link_IP	CM_MAC
ES_Global_IP	ES_MAC	CM_Global_IP	CM_MAC
State3			
ES_Link_IP	Malicious Server_ MAC	CM_Link_IP	Malicious Server_ MAC
ES_Global_IP	Malicious Server_ MAC	CM_Global_IP	Malicious Server_ MAC

2.2 Study 2

This study is IPv6 security issue using DAD procedure in Large-Scale Data Center.

Normally, when server first joins the IPv6 network and starts communication with other servers, it generates an IPv6 link-local address. And then, server checks IPv6 link-local address which is used address or not using ND message [6]. It is possible to makes paralyzed and confused to large-scale data center systems using this DAD procedure like Fig2.

① When Execute server3 join to IPv6 network, it should send NS message for DAD procedure.

② Malicious server sends fake NA message which is used IPv6 address to execute server3. After this, Execute server3 can't communication to others using this IPv6 address.

3 Conclusions and Future works

The aim of this study was to examine IPv6 security issue in large-scale data center. Many large-scale data centers actively adopt IPv6. There are many reasons why IPv6 have deployed in this filed: larger address space, SLAAC, Quality of Service (QoS), improved security and etc. Specially, SLAAC is a useful way of easily enabling IPv6 across your network. But SLAAC has drawbacks with respect to security of large-scale data center systems.

In this paper, we explained IPv6 security issues in large-scale data center. First thing is about modulated neighbor cache table and the other thing is about interference of DAD procedure. Through this, malicious server causes the system to become paralyzed or confused.

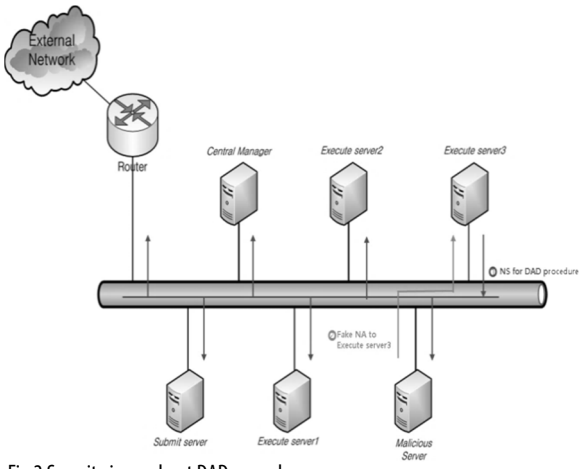

Fig 2 Security issue about DAD procedure

In the future plan, we plan to develop a system for protect large-scale data center systems even SLAAC environment of IPv6

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) through contract N-17-NM-CR01 and the Program of Construction and Operation for Large-scale Science Data Center (K-17-L01-C05).

REFERENCES

[1] J Bernier, S Campana et al, "The production deployment of IPv6 on WLCG," CHEP2015, 2015.
[2] S. Deering, R.Hinden, "Internet Protocol, Version 6 (IPv6) Specification," IETF RFC 2460, December 1998.
[3] Internet Engineering Task Force, http://www.ietf.org.
[4] Postel, J., "Internet Protocol", RFC 791, Sep. 1981.
[5] A S. Thomson, T. Narten, T. Jinmei, "IPv6 Stateless Address Autoconfiguration", IETF RFC 2462, September 2007.
[6] A. Conta, S. Deering, M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", IETF RFC 4443, March 2006.

Sangwook Bae received the MS and Ph.D degree in Computer Information Communication Engineering from Konkuk University, Korea in 2009 and 2014. Now, he is a senior researcher in Korea Institute of Science and Technology Information (KISTI) which is a national laboratory specialized to Information Technology, Korea. His research interests include batch system, IPv6, future network and security.

Heejun Yoon is principal researcher at National Institute of Supercomputing & Networking, KISTI. He received his M.S in Computer engineering from Univ. of ChungNam, Korea in 1997. His Research interests are HPC, Grid/Cloud Computing system, Large Scale Database and HPC training course.

Byungyun Kong received the MS degree in Particle Physics from Konkuk University, Korea in 2009. Now, he is a researcher in Korea Institute of Science and Technology Information (KISTI) which is a national laboratory specialized to Information Technology, Korea. His research interests include batch system.