Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2020, 7(1):140-146**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

SecRA 6 an algorithm to secure IPv6 Home Networks

Massamba SY[1], Cheikh SARR[1,2], El Hadji B. DIAW[1]*

[1]Laboratory of Science and Technology of Water and Environment (LaSTEE), Polytechnic School of Thies BP 10 Thiès, Senegal, (elhbdiaw@ept.sn*)
[2]University of Thies, UFR Sciences and Technologies, CitéMalickSy, PB 967, Thiès, Senegal

Abstract In this article we present a new algorithm that improves security of IPv6 home networks. With the introduction of version 6 of Internet Protocol, we see that the current trend in home network management is autoconfiguration (SLAAC) and the presence of several Internet service providers called Multihoming. This most certainly promotes vulnerabilities in the self-obtaining of an IPv6 address, a necessary condition for being part of a network due to the absence of a management system and control of this process of obtaining an address.

Our method propose an IPv6 security algorithm called SecRA6 (Secure Router Advertisement for IPv6) is used to authenticate router advertisements (RA) to secure the process of obtaining an IPv6 address in the home network. We used the ICMPv6 protocol to create two new packages called Neighbor Bandwidth Solicitation (NBS) and the Neighbor Bandwidth Advertisement (NBA) which used with the NDP protocol allows us to control autoconfiguration messages (RA) in order to authenticate the source. Thus after this verification we give the authorization to the routers to relay the RAs or to abandon them.

Keywords Algorithm, IPv6, ICMPv6, RA, NDP, NBA, NBS, Security, election, Homenet

1. Introduction

The new uses of the Internet as well as the development of home automation and artificial intelligence make the use of IPv6 [1] a necessity. This IP protocol version tries to correct the shortcomings of its predecessor IPv4 by introducing security natively in its datagram, but poses new security issues especially in home networks in which we note a lack of technical skills at the level of users.

In order to manage the neighborhood information, routers use the NDP [2] used in IPv6 nodes to discover other nodes on the local link to determine the information that a node needs to reach its neighbor. Using the Router Advertisement (RA) and Router solicitation (RS) packets of the ICMPv6 protocol [3] to manage the autoconfiguration of the hosts, NDP used with the IPv6 protocol stack is responsible for determining the link layer addresses of the various nodes. Target of most denial of service attacks, NDP because of its lack of security mechanisms, these flaws become a vulnerability in the automatic management of networks. With its role in the autoconfiguration mechanism, security mechanisms must be implemented to ensure robustness in this process of obtaining an IPv6 address.

The rest of the paper is organized as follows. Chapter 2 elaborates NDP Message and security issues of this protocol. In chapter 3, we presented the SecRA6 algorithm and in Chapter 4 presents the results and evaluation of system performance using various parameters and chapter 6 conclude this paper and discuss some possible approaches to optimize SecRA6 and provide some recommendations for SecRA6 deployment.

2. Work environment and related work

Several solutions for securing IPv6 networks are proposed in the literature, only rare are those that deal with IPv6 home networks and are not always easy to implement. In this paper, we will focus on the security issues related to obtaining an IPv6 address and the protocols that introduce techniques for autonomous network management. Most of them used the ICMPv6 protocol to develop knowledge management in order to allow protocols such as NDP to manage the local link.

According to the work presented in [4] and the ARBOR Networks 2011 annual report [5], the majority of attacks against IPv6 networks are of the DoS and DDoS type. In [6] O. E. Elejla, M. Anbar & B. Belaton present statistics on most attacks targeting IPv6 networks, we clearly see that DoS represent more than 70% of them. At the end of the 12th Worldwide Infrastructure Security Report [7] of ARBOR, the observation is that DoS or DDoS attacks are those which are at the top of the lists of attacks against Internet service providers.

2.1. NDP

NDP is one of the main protocols in the IPv6 suite. Defined in several RFCs, we will retain RFC 4861, the NDP protocol for IPv6 uses ICMPv6 packets for several critical functions such as the discovery of other existing nodes on the same link, finding routers, and retaining accessibility information on paths to the active neighbor, the determination of other link layer addresses, the detection of duplicate addresses. Others functions of NDP are the mechanism required to Accomplish, Prefix Discovery, Parameter Discovery and Address Auto configuration.

The neighbor discovery process is divided into two components. The first generally called Neighbor Discovery (ND) allows IPv6 nodes, on the same network link, to exchange information. It allows nodes to know the physical addresses, Link-Layer Address (LLA), associated with IPv6 addresses. At this stage of the process two ICMPv6 messages are used namely the NA and NS. The second, generally called Router Discovery (RD), allows information to be exchanged between an IPv6 node and an IPv6 router in which two other ICMPv6 messages are also used, namely RA and RS.

This process is the one used in SLAAC [8] to allow a node to obtain an IPv6 address.

In the case where we note the presence of fake RA in the networks due to a MiTD attack or a flood of Rogue RA, that would bring about bad configuration of the hosts that's causes vulnerabilities of the system and breakdown the network. Many solutions and the issues they fail to address have been summarized [6].

2.2. ICMPv6

ICMPv6 used with version 6 of the IP protocol brings significant changes compared to its predecessor ICMPv4. In both IPv4 and IPv6, ICMP provides error reporting, flow control, and gateway redirection. In IPv6, ICMPv6 has acquired a much more important and essential role due to the new functionalities now implemented via ICMP. Generic protocol, it can additionally report errors found in packet processing, perform diagnostics, perform neighborhood discovery, and report membership in a multicast. Essential in SLAAC autoconfiguration, it brings real changes in the autonomous management of IPv6 networks.

ICMPv6 packets are made up of fields: Type, Code & Checksum.

The 8-bit Type field indicates the type of message:

If the most significant bit is zero ***(value 0)***,
Return *Error message*: **Type [0 to 127],**
Else ***(value 1)***
Return *Information message:* **Type [128 to 255]**
End If

Depending on the type of message, the 8-bit Code field is used to create an additional level of message granularity.

The Checksum field is used to detect errors in the ICMP message inside an IPv6 packet.

NDP relies on ICMP to manage the neighborhood, so in order to secure the process, we will look at the solutions proposed in the literature.

2.3. SeND

The SeND [9] is a mechanism to protect against internal attacks. In [10] to protect the discovery of routers the SeND requires that the routers must be authorized to act as such. This permission is provided to both routers and hosts. Routers receive a RSA Signature option contain in Cryptographically Generated Addresses (CGA) from a Trusted Anchor, and hosts are configured with that Trusted Anchor to authorize routers. A CGA is an IPv6 address that has a host identifier computed from a cryptographic hash function. This procedure is a method for binding a public signature key to an IPv6 address in the SeND.

2.4. Rogue RA

The attacker sends RA periodically, pretends to be the last hop router and makes a statement on its lifetime value equals 0. The cheated host would consider that the router no longer provides services and therefore chooses the fake host as a default router. As a result, the attacker has opportunity to cutoff the victim's communication with hosts or complement man-in-the–middle (MITM) attack [11].

3. SecRA6

SecRA6 helps prevent bad or rogue RA. It operates before the address generation phase. Using NDP, it builds on through new ICMPv6 messages in view to construct a reliable database of different sources of router announcements.

So to secure this process, our technique which consists in controlling all the requests which are made to the routers for obtaining prefixes of auto configuration. In order to implement our defense mechanism (SecRA6), the first step of this process is the construction of the HomeNet domain, the second step allows to control the relay of auto configuration messages and finally the third will allow to take the decision to retransmit or not the RA messages

3.1. Step 1: Building the HomeNet domain

We rely on the creation of new ICMPv6 messages to organize the functioning of the home network. These new message types will allow us to encapsulate TLVs (length value type) in order to define metrics that allow us to organize the operation of the network by giving roles to each router. In accordance with the new specifications that provide ICMPv6 with more extensive functionality, we are using ICMPv6 packet types reserved for experimental purposes to implement our method. To establish the neighbor relationships, the nodes will use now NBS Neighbor Bandwidth Solicitation (icmp type: 200) instead of NS and the NBA Neighbor Bandwidth Advertisement (icmp type: 201) instead NA for the discovery of neighbors. To do this we define new rules in the exchanges between two nodes, which happen in three stages as illustrated in the figure 1.

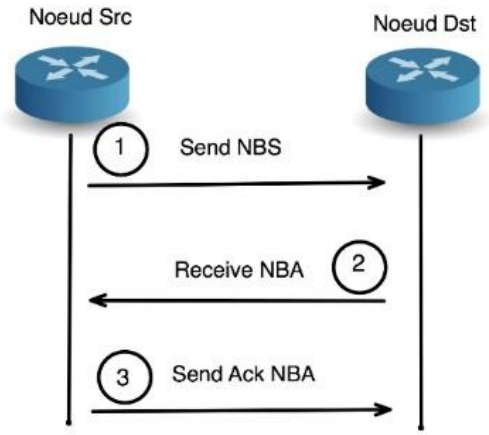

Figure 1: Neighborhood - 3-step exchange

NBS and NBA messages allow routers to build their neighbor list by sending each other their adjacency information such as identifiers (GUA and LLA addresses) and bandwidth information for uplinks to ISPs.

The addresses identifying the routers and the bandwidth information are used to perform the ascending sorting function to give the router a role in HomeNet.
The structure of the new NBS and NBA messages is very similar to those of the NS and NA, only we have introduced new fields of control in order to achieve the construction of the domestic domain.
The Structure of ICMPv6 NBS and NBA messages is shown in Figure 2.

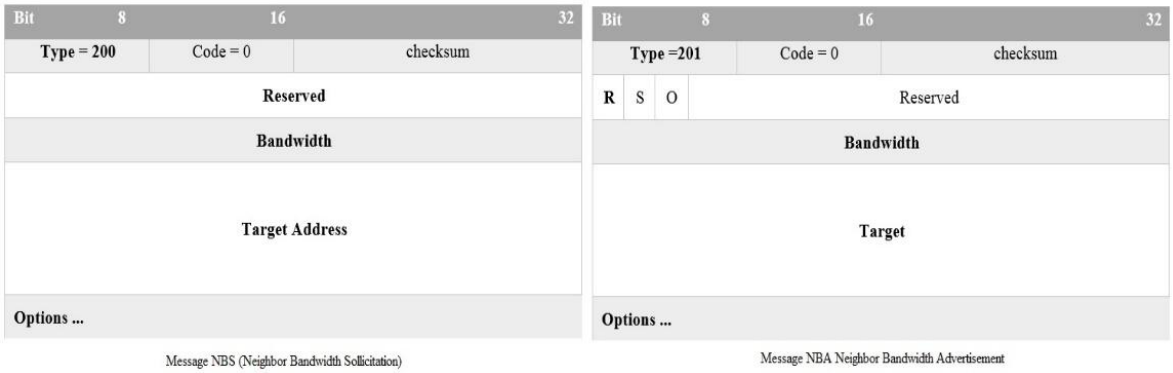

Figure 2: NBS and NBA datagram

Rules for using fields in NBA
The bit in the **R** field should contain the value 1 to specify that it is a router, otherwise the message will be abandoned.
The Bit in the **S** field should contain the value 1 to specify that the source of an NBA is always an LLA address.
The bit in the **O** field should contain the value 1 to specify that the destination of an NBA is always a multicast address FF02::2.
The information's collected through the sending and receiving of NBS and NBA allows the execution of a bandwidth sorting function on the TVL database to build different tables for the management of the domain, the most important of which are:

- the trust table or HTT (HomeNet Trusted Table) of possible sources of autoconfiguration messages
- and the HRRT (HomeNet Router's Roles Table)

3.2. Step 2: RA recovery function

With the listening function below, we use a method, which consists in stopping the relay of the RA message by setting the value of the Hop limit field to 1. This means that the packet can no longer be routed. But before stopping the packet, we make sure that it is an ICMP packet by making sure that the Next header field contains the value 58. After that we get the IPv6 prefix and the source address of the RA
At the end of this step we proceed to the validation of the source of the router advertisement (RA); if it is not indicated or not present in HTT, the router concludes that the source is unsecure, then it abandons the RA and the process ends.

3.3. Step 3: RA relay

If the address is verified as present in the HTT, the router re-encapsulates the Prefix in a new RA and returns it with the multicast address *FF02::1* to all hosts.

4. Results and Simulation

4.1. Working environment

In order to verify the results of the implementation of the SecRA6 algorithm, we used NS-3 in which we used the C++ language to develop the different functions that make up our algorithm. NS-3 is a discrete-event network simulator for Internet systems, targeted primarily for research and educational use. ns-3 is free software, licensed under the GNU GPLv2 license, and is publicly available for research, development, and use.

4.2. Results and interpretation

In order to implement our SecRA6 algorithm, we have developed three essential functions which have allowed us to test the results in order to check if they give satisfactory results.

4.2.1. Building Home network domain

We have built the NBS class which allows us to set up the HTT. With the listening functions of NBS and NBA messages, we recover the global IPv6 addresses, the local link address and the bandwidth of the uplink which contain the different information of which we need to build the domain.

Function 1 : Building domain with NBS an NBA.

```
TT (char Nom, long Ad_LLA, long Ad_GUA, long BW)
        {
 Nom = Nom ;
        AdD_L = Ad_LLA ;
        Add_G = Ad_GUA ;
        Bw_up = BW ;
 }
```

4.2.2. RA listening and recovery function

With the listening function below, we use a method which consists in stopping the relay of the packet by setting the value of the Hop_limit field to 1. This means that the packet can no longer be routed. But before stopping the packet, we make sure that it is an ICMP packet by making sure that the Next_header field contains the value 58. After that we get the prefix and the source address of the RA.

Function 2 :Recup Prefix and IP in RA

```
INPUT IP_Paquet
If Next_header== 58        // If icmp message the value is 58
 If Type== 134        // If the advertisement is an AR
          Hop_limit ← 1        // End of life of the message
          Tab.prefix ← Prefix // Getting the prefix
          Tab.Src ←Src_Address // Getting the source address
 Else Routing Fonction ()
 Endif
Endif
End
```

4.2.3. RA relay

In a first step we build an RA reception function which will allow us to extract the address with which the RA was sent. Can be a local link address, a global unique address or an unspecified address, it is extracted and compared with the addresses of the Homenet Trusted Table (HTT). The RA recovery function stops the relay processor by putting in the hop_limit the value 1 which will mean that the packet will stop at the node which is here a router (see Recup_Prefix function). The choice of the value 1 instead of 0 in the Hop_limit field is justified because the value 0 indicates on return that the default routing function is no longer possible, so with the value at 0, the packet would be destroyed

In the second step, we validate the source of the router advertisement (RA); if it is not filled in or not present in the Homenet trust table, the router concludes that the source is unknown, then it abandons the RA and the process ends. We present all the treatments in the RA_Relay function

Fonction3 : RA Relay

```
Relai_RA (Nœud Router, Paquet paquet, SBA Tableau) {
Int test←0
For (i ← 1 à TT.longueur )
 If (Tableau[i].GetAd==TT.SrcAdd) {// source verification
                Compute New_RA ()        //Encapsulates the prefix in a
                                                  // new message icmp type = 134
                                         //Define destination address to FF02::1
        test←1 ;                         // Test Control
        Break ; }                        // Stop loop }
Else{ i++ ;}
        EndIf
        If (test==0) {
        Hop_limit←0 }                    //Drop message
         EndIf
EndFor
```

5. Conclusion

In this article we have presented the SecRA6 algorithm for authenticating the source of an RA router advertisement. Whether it comes from an unspecified source "::" or from an internal or usurped source, AR cannot be relayed. We have presented the essential functions which make it possible to secure the process of obtaining an IPv6 address. The main objective of SecRA6 is to verify the origin of the RA in order to authenticate that the source is secure. Otherwise, the process of relaying router announcements is aborted. Through this solution we add a new vulnerability detection mechanism of the IPv6 protocol in addition to the techniques already proposed in the field

Compared to existing methods for detecting vulnerability of IPv6 concerning processes for automatically obtaining stateless IPv6 addresses, SecRA6 presents more flexibility and ease in view of the results obtained after its implementation. Based on a script, we run it once on the nodes and the process runs dynamically and autonomously and maintains a safe and easily manageable home environment.

Compared to SeND, SecRA6 is easier to implement and does not suffer from very large processor computation time due to the checks of certificates which are carried out by SeND hosts to ensure that announcements of neighborhoods are safe

In our future work, we plan to set up a version of SecRA6 with the use of cryptographic solutions to secure exchanges between the different nodes that use SecRA6. Operating at the level of peripheral routers, it presents a more interesting positioning in relation to the security aspects but does not use a cryptographic identifier to ensure greater security. So in our current work we are looking at how to integrate these aspects to give more scope to our solution.

References

[1]. S. Deering, R. Hinden., “Internet Protocol, Version 6 (IPv6) Specification”, IETF RFC 8200, July. 2017

[2]. T. Narten, W. A. Simpson, E. Nordmark, and H. Soliman, “Neighbor discovery for IP version 6 (IPv6),” 2007. RFC 4861 [online]. Available: https:// tools.ietf.org/html/rfc4861. Last accessed on 2019 September.

[3]. A. Conta, S. Deering, M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)" RFC 4443 Specification, Internet Engineering Task Force March 2006

[4]. Ali H. Nasser El Deen ‘’ICMPv6 Router Advertisement Flooding’’, https://www.researchgate.net/publication/266022049, Technical Report, December 2013

[5]. Arbor Networks’ 7th annual Worldwide Infrastructure Security Report, 2011

[6]. Omar E. Elejla, Mohammed Anbar & Bahari Belaton, "ICMPv6- Based DoS and DDoS Attacks and Defense Mechanisms: Review", IETE Technical Review, Aug 2016
[7]. Arbor Networks' 12th annual Worldwide Infrastructure Security Report, 2016
[8]. S. Thomson, T. Narten, T. Jinmei, "IPv6 Stateless Address Autoconfiguration (SLAAC)" RFC 4862 Specification, Internet Engineering Task Force September 2007
[9]. J. Arkko (Ed.), et al., "SEcureNeighborDiscovery (SEND)", IETF RFC 3971, March2005
[10]. Chown, T., Venaas, S., "Rogue IPv6 Router Advertisement Problem Statement", IETF RFC 6104 (Informational), Feb. 2011
[11]. J. B. Ard, Internet Protocol Version Six (IPv6) at UC Davis: ''Traffic Analysis with a Security Perspective''. Davis (CA): University of California, Davis, 2012.