Presented at the DLSU Research Congress 2015
De La Salle University, Manila, Philippines
March 2-4, 2015

# IPv6 Stateless Address Autoconfiguration (SLAAC) Attacks and Detection

Franz Justin Buenaventura, John Paul Gonzales, Matthew Emanuel Lu and Arlyn Verina Ong*
*Center for Networking and Information Security, De La Salle University*
*Corresponding Author: arlyn.ong@delasalle.ph*

**Abstract:** In order to sustain its exponential growth, the Internet community is gradually transitioning from its mainstream communications protocol Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6). IPv6 provides a virtually inexhaustible address space, capable of accommodating the hundreds of billions of unique devices. Through a procedure called Stateless Address Autoconfiguration (SLAAC), IPv6 also provides a network device the capability to automatically set its own Internet address. While providing this convenience, SLAAC possesses several vulnerabilities in its design. The top three common attacks against the IPv6 SLAAC mechanism, namely the malicious last hop router, neighbor spoofing, and duplicate address detection denial of service attacks exploit these vulnerabilities This paper discusses detection methods for these attacks, implemented using a system that captures network traffic, and monitors IPv6 SLAAC operations through examination of discrepancies between expected network settings and SLAAC messages sent between devices in the network. To test these detection methods, the system is set up to monitor an IPv6 network and the three attacks are performed against network hosts. Results show that the system is capable of detecting SLAAC attacks within seconds from attack onset across multiple trials, thereby demonstrating that data traffic monitoring is a viable solution for mitigating the security issues that SLAAC may cause in an IPv6 network.

**Key Words:** IPv6; network protocols; network security

## 1. INTRODUCTION

In the past two decades, the Internet has experienced a very rapid rate of expansion as the number of connected devices grew exponentially (Internet Live Stats, 2014). During this period of rapid growth, Internet Protocol version 4 (IPv4) serves as the communication protocol used by the global Internet. IPv4 was designed to as a communication medium-independent protocol capable of supporting up to four billion devices through its IP addressing system. This limited pool of addresses is insufficient to continue supporting the large number of Internet users today, which numbers at more than 3 billion. While there are available address conservation strategies in use such as private addressing and Network Address Translation, these will be inefficient in the long run as the number of Internet users is expected to continue growing exponentially. It is predicted that there will be approximately 25 billion devices connected to the Internet by the year 2020 (Barker, 2014). In

contrast, as of February 2011, the IPv4 address pool is already considered exhausted, with less than 70 million addresses still available (Huston, 2014).

With the depletion of public IP addresses available from IPv4, Internet Protocol version 6 (IPv6) was developed as a next generation Internet Protocol. IPv6 expands the available pool of addresses to about 3.4 undecillions (Cisco Systems, 2011), creating a virtually inexhaustible address space, and allowing a multitude of devices to be connected to the Internet. IPv6 also introduces a unique feature previously unavailable in IPv4 – the capability of devices to select their own IPv6 addresses using the Stateless Address Auto Configuration Protocol (SLAAC).

The SLAAC mechanism allows the automatic address configuration of network devices without the need for a central server. This reduces the requirement for device address tracking and central address management in an IPv6 network, further positioning IPv6 as a protocol that is capable of handling communications for a large number of devices. The design of the SLAAC mechanism however, presents vulnerabilities that make it susceptible to attacks designed to prevent devices from successfully generating their own IPv6 address. If these security issues are not addressed, adoption of the SLAAC protocol may be hindered in spite of the convenience that it provides to the management of a network.

This research aims to provide methods by which attacks against the SLAAC protocol may be monitored in an IPv6 network. This paper first discusses the design of SLAAC as well as methods of attacks against it. It then discusses methods by which attacks may be detected and the results of testing these techniques. Finally, it presents the findings from the tests and future work for the research project.

## 2. STATELESS ADDRESS AUTO-CONFIGURATION

The Stateless Address Auto-configuration (SLAAC) protocol generates addresses using the network prefix of the logical network to which a host belongs, and a self-assigned identifier for the network interface of the host.

### *2.1 SLAAC Procedures*

To acquire needed information about the network and ensure address uniqueness, SLAAC uses Neighbor Discovery Protocol (NDP), a group of control messages (Thompson et al, 2007). NDP uses four messages types to support SLAAC procedures. Upon connection to a network, a device uses a Router Solicitation Message (RS) to contact the network gateway router. The router responds with a Router Advertisement (RA) bearing the 64-bit prefix of the network. It should be noted that RAs are also periodically broadcasted by the gateway regardless of solicitations from network members. Upon receipt of an RA, the connecting device generates a 64-bit host identifier either randomly or from the Media Access Control (MAC) address associated with its network interface. This identifier is then appended to the network prefix obtained from the router to form a tentative 128-bit IPv6 address for the host.

In order to verify the uniqueness of the generated address within the network, the device must perform the Duplicate Address Detection (DAD) procedure. It issues a Neighbor Solicitation (NS), a message that is used in IPv6 networks to query for the MAC address of a target host given its IPv6 address. When used in SLAAC procedures, a device sends this message querying for its own IPv6 address. This effectively tests for the presence of another device on the network that may coincidentally have the same IP address. If there is no reply to the query, then the device assumes that the generated address is unique and proceeds to use it for communication. If it is not unique, the existing host bearing the same address returns a Neighbor Advertisement (NA) message; and the device must repeat the address generation and DAD process.

### *2.2 Security Issues and Attacks*

The relatively simple method by which SLAAC operates shows that on a device attempting to generate an address, there is no verification done on RA and NA messages it receives from the network. This makes a device susceptible to cases where maliciously crafted RA and NA messages may prevent the host from successfully generating an address for itself, effectively preventing it from communicating on the network it intends to join, or allowing its data traffic to be intercepted.

The Malicious Last Hop Router is an attack that involves a malicious host posing as the legitimate router on the network (Nikander et al 2004). In this attack, the bogus router sends illegitimate RAs to the network in order to force other network hosts to use a different network prefix. This causes the hosts to use the bogus router as the network gateway, resulting to data traffic being directed to the bogus router instead of the legitimate one. In effect, this allows the bogus router to freely intercept any data sent from other members of the network; or to cause a denial of service in the network by stopping data from travelling to other networks through the legitimate gateway.

Neighbor Advertisement Spoofing, is an attack wherein an attacker makes a custom NA message that advertises its own MAC address as the gateway (Stretch, 2009). Similar to the effect of the Malicious Last Hop Router Attack, it allows an attacker to intercept data that should be directly sent to the legitimate gateway. The main difference is that in this attack, the IPv6 address of the legitimate router is known to victim host; however, it is mistakenly mapped to the MAC address of the attacker. When the victim sends data meant for the gateway, it is first transparently directed to the attacker who can read the data before forwarding it to the gateway.

Denial of Service attack in Duplicate Address Detection also known as DoS in DAD, is an attack that allows an malicious host to prevent a host on an IPv6 network from obtaining an IPv6 address (Grunter et al., n.d.)When an intended victim attempts to perform the DAD process, the attacker can reply with an NA message for each NS that the victim sends in the network. This causes the victim to keep assuming that the addresses it generates are already in use. This continues until the victim eventually stops initializing its interface and fails to connect to the network.

## 3. DETECTION SYSTEM FOR IPv6 SLAAC ATTACKS

To detect ongoing attacks against the SLAAC protocol in a network, this research proposes a system that monitors NDP messages transmitted among hosts. The system must be deployed with a connection to a trunk port on the network switch as in Fig. 1 to be able to sniff out relevant NDP messages, which are sent as multicasts on the network.

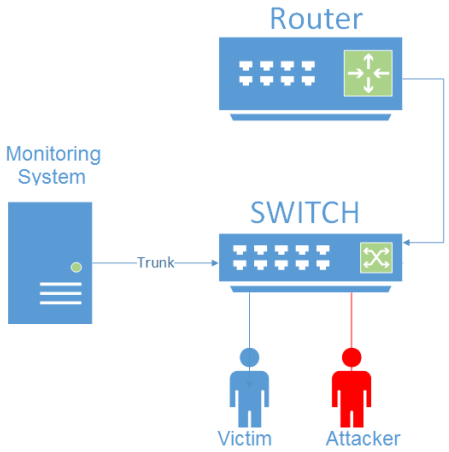


Fig. 1. Detection system network topology

The system collects Router Advertisement (RA), Neighbor Solicitation (NS), and Neighbor Advertisement (NA) for parsing and inspection. It also builds a router database which contains the list of legitimate router addresses.

Detection of the attacks mentioned above requires different approaches which are discussed in the following subsections.

### *3.1 Malicious Last Hop Router Detection*

The system utilizes its router database to detect the presence of a malicious router. When building the router database upon system setup, the link layer address and IPv6 address of each legitimate router expected on the network must be listed. Once the system is operational, RA messages are captured and parsed. The contents of the RA is compared against the router database according to the algorithm in Fig. 2.

```
router_db=get_router_db()
if packet_type == RA
{
  for x in router_db_len
  {
  if(packet_link_add != router_db[x])
    //Malicious RA
  else
    //legit RA
  }
}
```

Fig. 2. Malicious RA detection algorithm

The source link layer address of the RA is compared to the source link layer address of the routers found in the database. This is to determine if the RA is from a known legitimate router or not. Should a matching address be found, then the RA is legitimate; otherwise, the RA is considered part of an attack and an alert is generated.

### *3.2 Neighbor Advertisement Spoofing Detection*

The detection method used for the second attack also requires the use of the router database. When the system receives an NA message, the target address of the message is examined according to the algorithm in Fig.3.

Since NA messages are regularly used even by non-gateway devices on the network, the router flag, override flag and the source IPv6 address of the captured message must be checked first in order to distinguish NA messages of other devices from that issued by the gateway. The router flag and override flags are checked to ensure that the NA is from a router while the IPv6 address is checked to verify that the router from which the NA came from is legitimate. If the NA contains the gateway IPv6 address, the corresponding link layer address contained in the NA message is compared against the entries recorded in the router database.

```
router_db=get_router_db()
if packet_type == NA
  {
     for x in router_db_len
       {
         if(router_flag==True and override_flag==True)
            {
               if(packet_src_add== router_db_src_add)
                {
                 if(packet_link_add != router_db[x])
                    // Spoofed NA
                 else
                    // Legit NA
                }
            }
       }
  }
```

Fig. 3. Neighbor spoofing detection algorithm

This is to make sure that the NA with the address of the router contains the address of the legitimate router. If both the source link layer address of the NA packet and the source link layer found in the database are equal, the NA is legitimate; otherwise, it is considered an attack.

### *3.3 Denial of Service in DAD Detection*

The third attack disrupts DAD attempts from hosts in order to prevent them from obtaining an address in the network. The algorithm used to detect this attack tracks DAD attempts in a database containing the time when the DAD attempt is made and the source link layer address of the attempt made

When an NS message is received, the source IPv6 Address of the NS is examined. The source address of the NS should be "::", a black IPv6 address indicating a DAD attempt. The system updates its DAD attempt database by recording the system time and the source link layer addresses of the attempt. After updating the attempts database, the algorithm deletes any recorded entries that are two seconds more than the system time, as these are considered obsolete attempts. Once the old attempts are deleted, the algorithm finds the first and last DAD attempts associatedwith the host sending

the NS, as well as the frequency count and stores it in a list.The time difference between the earliest and latest attempt is then calculated. If this difference is less than one second, and the attempt frequency count is more than two, this indicates a host that has repeatedly attempted unsuccessful DAD procedures and is flagged as an attack. A. summary of this procedure is illustrated in Fig. 4.

```
if packet_type == NS
{
  if(source_add==":")
  update_attempt_db(packet)
  delete_old_attempt()
  address_list=[]
  open_file(attempt_db)
  foreach(line in attempt_db)
  {
    flag= false
    if(address_list is empty)
    {
      new_ent=package(details)
      address_list.append(new_ent)
    }
    else
    {
      if packet_add == address_list_ent
          address_list.update
          flag= true
      if not found
          new_ent=package(details)
          address_list.append(new_ent)
    }
  }
}
foreach(ent in address_list)
{
  count= ent[5]
  time_f=get_timestamp_first(ent)
  time_l=get_timestamp_last(ent)
  diff = time_f -time_l
  if ( diff <=1 and count >2)
      //Attack Detected
  else
    //DAD Legitimate
}
```

Fig. 4. DoS in DAD detection algorithm

## 4. SYSTEM EVALUATION

The implementation and the testing of the system uses a network setup of three host computers: one serving as an attacker, another as the victim, and the third as the PC hosting the system. A packet monitoring system is deployed in the attacker and the victim hosts in order to observe the network activity.

For each attack, a set of pre-programmed IPv6 packets are sent on the network with the system deployed to test if attack packets can be successfully detected by the system. For each trial, the detection time is calculated by noting the arrival time of the attack packet to the time it was flagged by the system.

### *4.1 Malicious Last Hop Router Detection Test*

The Malicious Last Hop Router Attack is simulated by sending a legitimate Router Advertisement with a lifetime of 0. This is to force any existing device configurations to expire and have devices accept new RAs. This is immediately followed by an illegitimate RA from the attacker. For this test, a total of 5 trials were run, each having a set of 35 mixed illegitimate and legitimate RAs. The system was able to detect all of spoofed and legitimate RAs. The summary of the test is shown in Figure 5.

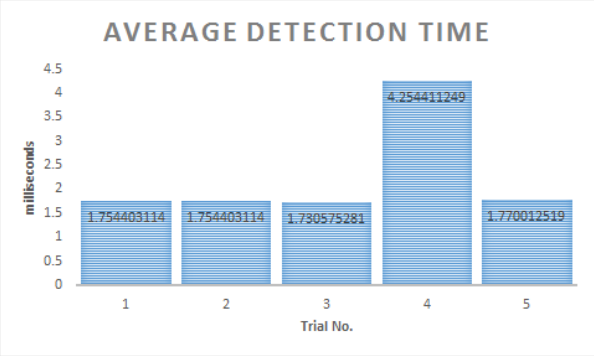


Fig. 5. Malicious Last Hop Router Detection results

The average detection time from sniffing, parsing, to detecting packets is approximately 2 milliseconds. As shown in figure 5, trial no. 4 had an unusually longer time of detecting compared to the others. This is assumed as a minor discrepancy from each trials of attack that may have been the result of computers performance in that given trial. Based on the test performed, the algorithm used is accurate as the system was able to

differentiate the spoofed RA and legitimate RA packets respectively.

### *4.2 Neighbor Spoofing Detection Test*

To simulate a Neighbor Advertisement Spoofing attack,the attacker waits for neighbor advertisements (NA) from the gateway of the network. When it detects an NA, the source address of the message is copied, with the solicited flag replaced with a router flag. The source link layer address in the packet is then replaced with that of the attacker. This is to allow the attacker to assume the identity of the gateway router. There are a total of 26 NAs that are received composed of of 18 legitimate and 8 attack packets for each trial..The summary of the test are shown in Fig. 6.

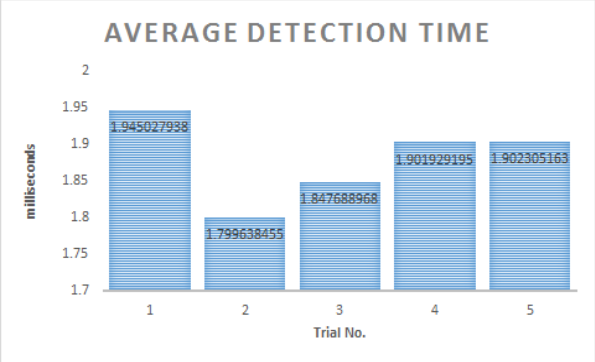


Fig. 6 Neighbor Advertisement Spoofing results

The average time of detection from the time that the packet is captured from the network to the time that it is alerted as an attack is less than 2 milliseconds. There are minor discrepancies from each attack that may have been result of computers performance in that given trial. From the test we also concluded that the given algorithm is accurate, the system only detected the attackers packet and ignored the legitimate packets that have been sniffed.

### *4.3 DoS in DAD Detection Test*

To simulate the DoS in DAD attack, the attacker is made to sniff an NA and if detected to be a DAD attempt, it proceeds to inform the victim via an NA message that the address sis in use. The setup to generate a DAD attempt is to create a new virtual machine with the network bridge and install Windows 7 for each trial. In each trial, the attacking machine generated between 9-20 NA messages. Fig. 7 illustrates the average detection time per trial.

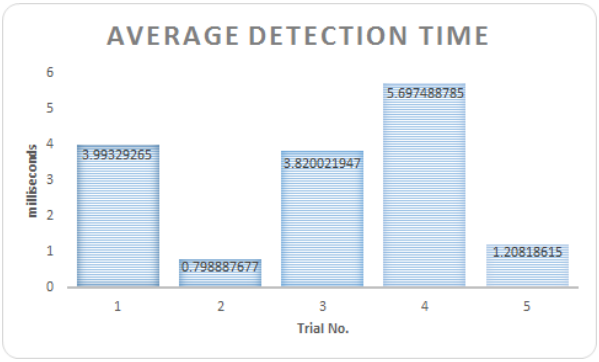


Fig. 7. DoS on DAD results

Based on the results the average detection time has big gaps with each trial. This may be due to the multiple detection entries of DoS in DAD for each trial. In addition, each trial produces a different set of attack packets. In a live network, the attempt count and the time limit for the algorithm for the detection should be adjusted depending on the network environment. There are external variables like network congestion, network size, and monitoring system performance that may affect the processing speed of the system.

## 5. CONCLUSIONS

In this paper, three attacks against the IPv6 SLAAC protocol were presented as well as corresponding methods for detecting the occurrence of these attacks in a network. The detection methods involved the monitoring of Neighbor Discovery Protocol messages transmitted within a network through a switch trunk port and the tracking of legitimate gateway router identities. Based on tests, these approaches are proven to be successful in detecting attacks within a few seconds from onset. This shows that packet

monitoring provides a viable solution for mitigating SLAAC attacks in an IPv6 network; however, the accuracy of results may be high at this point due to the lack of variation in attack pattern. As such, the system algorithms are tailored to detect for these known patterns only. Should there be new methods to accomplish the same attack, then these may undetected in the network.

As future research, the system will be extended to provide the capability to not only detect, but to also respond to an attack by correcting the device configuration errors induced by an attack, or by implementing changes to network configuration to temporarily halt the effects of an attack.

## 6. REFERENCES

Barker, C. (2014). 25 billion connected devices by 2020 to build the Internet of Things. ZDNet (ZDNet)http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/

Cisco Systems. (2011). Overview of IPv6. Routing and bridging guide vA5(1.0), Cisco ACE Application Control Engine. Cisco Systems Inc. 2, 1-14.

Grünter, E., Anrath, W. &Werner, S. (n.d.) Securing IPv6: neglected IPv6 features. Admin Network and Security. http://www.admin-magazine.com/Articles/Neglected-IPv6-Features

Huston, G. (2014). IPv4 Address Report (IPv4 Address Report)http://www.potaroo.net/tools/ipv4/

Internet Live Stats (2014) Number of Internet Users (2014). http://www.internetlivestats.com/internet-users/

Nikander, P., Kempf, J. &Nordmark, E. (2004). IPv6 neighbor discovery (ND) trust models and threats. RFC 3756. IETF.

Stretch, J. (2009). IPv6 neighbor spoofing. Packet Life.net http://packetlife.net/blog/2009/feb/2/ipv6-neighbor-spoofing/

Thompson, S., Narten, T., &Jinmei, T. (2007). IPv6 stateless address autoconfiguration,RFC 4862. IETF.