ijecs
open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9, September 2014 Page No. 8445-8459

IPV6 SLAAC related security issues and removal of those security issues

Priya Tayal
M-TECH student of Computer Science & Engg
ABES Engg College,Ghaziabad
Priyatayal1991@gmail.com

Abstract: The internet protocol version 4 (IPV4) is depleting in address spaces day by day and hence the deployment of IPV6 in network is very essential. IPV6 is a new generation protocol that is expected to solve the issues that arise in IPV4 but also poses some security issues. The emphasis in this paper is to identify the vulnerabilities that come in IPV6 and how to remove those vulnerabilities. Reconnaissance attack is employed by attackers to fraudulently enter in IPv6 network. For this reason an unique and secured IPV6 address will be generated so that a secured network can be set up and malicious nodes would not enter the network. There are different type of techniques that are used like i-SeRP(IPV6 Security Risk Prototype), CGA(Cryptographically Generated addresses), Privacy Extension, SSAS (Simple Secure Addressing Scheme) to make the network secure. In this paper an unique secured IPV6 address will be generated to make network secure by using the combination of certification authority and PKI structure for node verification, Diffie Hellman for exchange of secrets.

Keywords: IPV6, Security issues of IPV6, SLAAC, Security Methods, Certificate authentication, Diffie Hellman. .

1. Introduction

IPV6 was firstly introduced by IETF (Internet Engineering Task Force) in mid 1990's. IPV6 is a next generation protocol that try to overcome the problems due to IPV4. IPV6 provides 128-bit address space that is 3.4*(10)^38 addresses. This address space is very large(its in trillions in trillions)[1].IP address is formed by the combination of the subnet prefix and and the interface ID. Subnet prefix composed the leftmost 64 bits of the address and IID composed the rightmost 64 bits of the address. In this paper rightmost 64 bits are trying to be generated uniquely. As migration from IPV4 to IPV6 is taken place ,there are some security issues that arise. Some are due to IPV4 and some are due to IPV6. In this paper firstly explaination of the problems related to the current mechanism will be discussed and then composed solution will be described.

The remainder of this paper is organized as follows- section II will define SLAAC(Stateless Address Auto configuration) and related security issues briefly. Section III will define the features of IPV6 over IPV4. Section IV will define techniques to removed the vulnerabilities caused by IPV6 SLAAC. Section V will define the problem statement. Section VI will evaluate the proposed solution and last section VI will conclude all the things.

2. What is SLAAC

SLAAC(Stateless Address Auto Configuration) is an unique feature of IPV6 for generating IP addresses automatically for large organizations [6]. It does not need any human intervention. As soon as a node joins a network, it configures its IP address. Thus it works in a "Plug and Play" fashion. It is used with other mechanism ND(Neighbour Discovery) to discover their neighbor routers and hosts. ND and SLAAC together can be termed as NDP (Neighbour Discovery Protocol). By using NDP, nodes on the network may get the information about the routers and process DAD (Duplicate Address Detection)[12].

In the network, communication between nodes takes place by exchanging messages- router solicitation (RS) message, router advertisement (RA) message and neighbor solicitation (NS) message[13]. When a host joins a network ,it sends a RS message to the router and then router reply by sending RA message containing their prefix. To avois conflicts on the network host processes DAD (Duplicate Address Detection)[12] by sending NS message.

By using SLAAC it imposes many security risks that are as follows-

A. Reconnaissance attack

Attackers may get information about host and network devices and their interconnection in the targeted network by using two methods- ACTIVE and PASSIVE methods. In the active method intruders do scanning of the data and in the passive method they fetch the essential data about the enterprise network[2] .

B. Denial Of Service(DoS) Attack

As intruders split the packets into small size of fragments so it will send large number of fragments to the target system until it become overload and crash the system.

C. Malicious router

As IPV6 use SLAAC for autoconfiguration of IP address so a malicious router may decide to serve as a legitimate router and misguides the packets in the network.

D. Failure of DAD and NUD processes

A malicious router may falsely respond to DAD (DuplicateAddress Detection) and prevents new nodes to join the link thus results in false NUD (Neighbour Unreachability Detection)[4].

3. FEATURES OF IPV6 OVER IPV4

There are a number of reasons why IPV6 is trying to take place over IPV4. IPV6 provides many features in comparison to IPV4.Some features provided by IPV6 is decribed below [2][3].

- IPV6 provides 128 bit address space while IPV4 provides only 32 bit address space. Thus IPV6 meet the requirement of network easily.
- IPV6 provides anycast addressing while IPV4 provides broadcast addressing.
- IPV6 uses SLAAC(Stateless Address Auto Configuration) i.e. unique to IPV6.
- IPV6 provides end to end connectivity so it does not use NAT(Network Address Translation) protocol while IPV4 make use of NAT.
- IPV6 removes 3 fields (Flag, Fragment offset,Identification) from header, that are used in IPV4.
- Packet fragmentation and reassembly of packets are done by sender and receiver host only in IPV6.
- IPV6 provides autoconfiguration by using NDP (Neighbour Discovery Protocol). Thus reduces the overhead of manual configuration of IP addresses.
- IPV6 provides path MTU(Maximum Transmission Unit) discovery.
- IPV6 provides flow labels and traffic classes for QoS(Quality Of Services).

4. TECHNIQUES TO REMOVE THE VULNERABILITIES CAUSED BY IPV6

There are a number of technologies already exist which try to reduce the security issues that arise in the network by using IPV6. Some techniques analyzes what type of router should be used so that less security issues arise and some try to use different types of algorithms to reduce those security issues. Thus existing technologies and there limitations are described below-

A. I-SeRP

In this it measures the potential security risk in the enterprise network by using IPV6 security risk prototype (i-SeRP) system[7]. Threats and vulnerabilities are identified by threat model and i-serp system helps the administrator in identifying the security risks and also in decision making approach for security policy. In this it does the risk assessment. There are three concept of risk assessment-

1. concept of vulnerability,
2. concept of threat,
3. countermeasure.

It uses three tables- table for threat value, table for vulnerability value and table for asset value determination[7].

RISK VALUE= SUM (Threat Value* Vulnerability Value) *Asset Value

THREAT MODEL

Threat model is used to identify the threats in the enterprise when deploy IPV6 and group the threats into the protocols. It identify the threats in the network layer. Then threats are categorized according to protocols that are directly affected. In this paper, attacks are described based on its severity ,likelihood of attacks and how it affects the network[8].

I-SeRP explains the calculation of the risk value which is described above. It follows several steps-

- Enterprise may choose whether router or switch to know its risk value when IPV6 is deployed.
- After asset is choosen router code and router price have to be entered.
- By using router codes enterprise may differentiate between the routers that are identical and are of same series.

Thus by entering the values from the tables and by calculating the risk values for each router, a table is made

.EXAMPLE OF RESULT OBTAINED BY I-SERP MODEL.

Num	Router code	Router series	Router price	Average risk value
1	1001	700 series dial-up	2055.41	86
2	1002	760 series dial-up	2055.41	86
3	1003	3900 series	45589.54	409
4	1004	7200 series	760008.96	491
5	1005	Catalyst 6608 series	63324.96	491
6	1006	11000 series	25320.48	245
			Total-	1808

From the table we may conclude that CISCO-7200 series router and CISCO- 6608 series router has the highest risk value[7]. Thus these routers are vulnerable to all possible threat protocols. Thus threat model identify the security risks that may effect the organization and i-SeRP measure the risk. By using this enterprise may evaluate the security risk of their assets and choose the right security mechanism to counter this risk.

B. EUI-64 Method

Standard method of generation of IP interface IDs (IID) is Extended Unique Identifier(EUI-64) i.e. offered by IEEE Standard Association[6]. EUI-64 is the combination of OUI

(Organizationally Unique Identifier) assigned by IEEE RSA and the extension identifier assigned by hardware manufacturer.

Limitation of this approach is that it generates same IID whenever a node joins a network. So it make intruders easy to track the node.

Two different techniques that generate the random IIDs

- CGA (Cryptographically Generated Addresses
- Privacy Extension Approach

C. CGA(Cryptographically Generated Addresses)

In this method a cryptographic public key is attached with IPV6 address in SeND (Secure Neighbour Discovery) protocol to generate random interface IDs. The resulted IPV6 address is called CGA[9]. For security point of view corresponding private key is then be used to sign message sent from the addresses. In this interface identifier is generated by computing a cryptographic hash function from a public key and an auxiliary parameters. CGA is the concatenation of modifier,subnet prefix,collision count, public key and optional extension fields. CGA is computed by using 9 step algo defined in rfc-3972 and can be verified by recomputing the hash value and by compairing the hash value with identifier.

CGA prevents spoofing and stealing of existing IPV6 addresses.

First limitation of this technique is that protection works without a certification authority. So an attacker can create a new address from an arbitrary subnet prefix and its own public key.

Second limitation is that there is no method to prove that the address is not CGA so an attacker can take anyone's CGA and present it as a non-CGA.

D. Privacy Extention Approach

This is an another method of randomly generating IIDs.

In this interface identifier is derived from IEEE identifier. By using this identifier a node can generate a global scope address that changes over time. Thus it make difficult eavesdropper and other intruders to identify the addresses as different addresses are used in different transaction. It uses two methods for the generation and maintenance of randomize interface identifier[10].

First in the presence of stable storage and second in the absence of stable storage.

When stable storage is present

it assumes the presence of 64-bit "history value" i.e. used as an input to generate the random IID using MD5 algo. When a system boots first time a random value should be generated and saved to the history for the next iteration of the algo.

When stable storage is absent

In this it uses configuration information like user identity, security key, serial number to generate some data bits and append some random data and compute the MD5 digest as before.

In this ingrees filtering is used to prevent the use of spoofed the source address in the distributed DoS attacks.

Limitation of this approach is that it prevents privacy related issues but not security related issues.

E. SSAS(Simple secure Addressing scheme)

To overcome the limitation of CGA and Privacy Extension Method, SSAS method is derived. SSAS[11] method is very simple and very secure. The main concerns in the previous approaches were the problem with generating current IID needed intensive processing and lack of security. As we all know that a node generate an address and keep it for a short time, so in this approach it do just like that. SSAS is a combination of randomly generated IID with a signature that is added to NDP message. This approach decreases the complexity of IID generation and mitigate the attacks against a NDP enable node.

SSAS include many steps to provide security and to generate random IID. Steps are following-

a) SSAS interface ID (IId)generation
b) SSAS signature generation
c) Generation of NDP message
d) Resource public key infrastructure (generation of RPK & SPK and processing of RPK & SPK).

a) SSAS interface ID generation

- Firstly generate key pairs.
- Divide the public key array of bytes into two half byte arrays i.e. partial IID.
- Concatenate partial IIDs and call it a IID .
- Concatenate the IID with local subnet prefix to set local IP address.
- Concatenate the IID with router subnet prefix to set global IP address.
- This is a tentative IP. To make it permanent DAD (Duplicate Address Detection) is performed.

b) SSAS signature generation

- Concatenate the timestamp with MAC address, collision count, algorithm type and global IP address.
- Then sign the resulting value from the above procedure using the ECC private key and the resulting signature is called SSAS signature.

SSAS signature is added to NDP message to protect them from IP spoofing.

c) Generation of NDP message

To prevent collision attacks in the network we do DAD (duplicate Address Detection). For this node generates a neighbor solicitation(NS)message. SSAS data field contains type, length, reserved, algorithm type, SSAS signature and padding. All NDP message should contain SSAS signature because it allows receiver to verify the sender. In response to a NS message,it gets a NA message for verification.

d) Resource Public Key Infrastructure(RPKI)

RPKI is used in the network to verify the authorized router and to maintain the trust. SSAS proposed the use of control node(CN). Administrator will be able to store it manually in the database and the router public key and MAC addresses. SSAS introduce two different NDP message – RPK(Request Public Key) and SPK(Send Public Key).

The NDP message type used for RPK is 140 and for SPK is 141.there are two new types in these messages- type 16 and type 17. Type 16 is used to generate a new IP address or to change IP address while type 17 is used for node's new public key.

Advantage of SSAS

- It prevents replay attacks by making the comparison of public key by its own key and by making use of timestamps.
- It prevents DoS attacks by monitoring a niode in the network.
- It prevents malicious router attack by SSAS verification process and by NUD(Neighbour Unreachability Detection) probes.
- It prevents IP spoofing by making use of SSAS verification process.

Limitation-

- Long computational process.

5. PROBLEM STATEMENT

The main problem is to find out the malicious node in the network.A unique technique is required to find out that malicious node with some technique. The main problems related to SLAAC are-

- Reconnaissance attack
- Malicious router
- Denial of service attack (DOS)
- Failure of NUD and DAD process

6. PROPOSED SOLUTION

In the proposed solution, IP will be fetched by SLAAC and then will be verified by CA(Certification Authority) and PKI (Public Key Infrastructure). Then IP will be secured by using Deffie Hellman key exchange algo. And after that existence of nodes in network will be verified by sending periodic probes. Description of the proposed solution is organized as follows- Section A will define the Algorithm of proposed solution, section B will define "What is Deffie Hellman Key Exchange Algorithm", section C will define will define the Certificate authentication and in the last, section D "Flow Chart" of proposed solution

A- Algorithm

1- Obtain IP address bits by SLAAC.

2- New node 'A' sends a "certificate" to CN(control Node) for the verification.Verification will be done by the CN through Certification authority(CA) as described in sec-B.

3- CN will make use of "PKI"(Public Key Infrastructure) for the verification. Thus if a node that enters in a network is not genuine then it will be discarded by the certification authority. And only the genuine node will proceed for the further processing.

4- CN will generate a unique rightmost 64 bit valid pattern and update it in the database.

5- Keys will be exchanged between genuine node and CN through "Diffie Hellman Key Exchange Algorithm".

6- CN will encrypt that rightmost 64 bit pattern using that secure key and send it to genuine node.

7- Genuine node decrypt that 64 bit valid pattern and generate a unique 128 bit address by combining leftmost 64 bit address to this rightmost 64 bit address.

8- 'CN' sends periodic probes to all nodes to know their existence in the network.

9- Probes will be encrypted by security key and including field COUNT.

10- Nodes will decrypt that probe and send REPLY by COUNT+1

11- If
nodes reply and reply match the pattern
it means these nodes are genuine and still in working phase in the network.
Else if
Node is not genuine or has completed its work and left the network.

12- Remove that IP address from the databse.

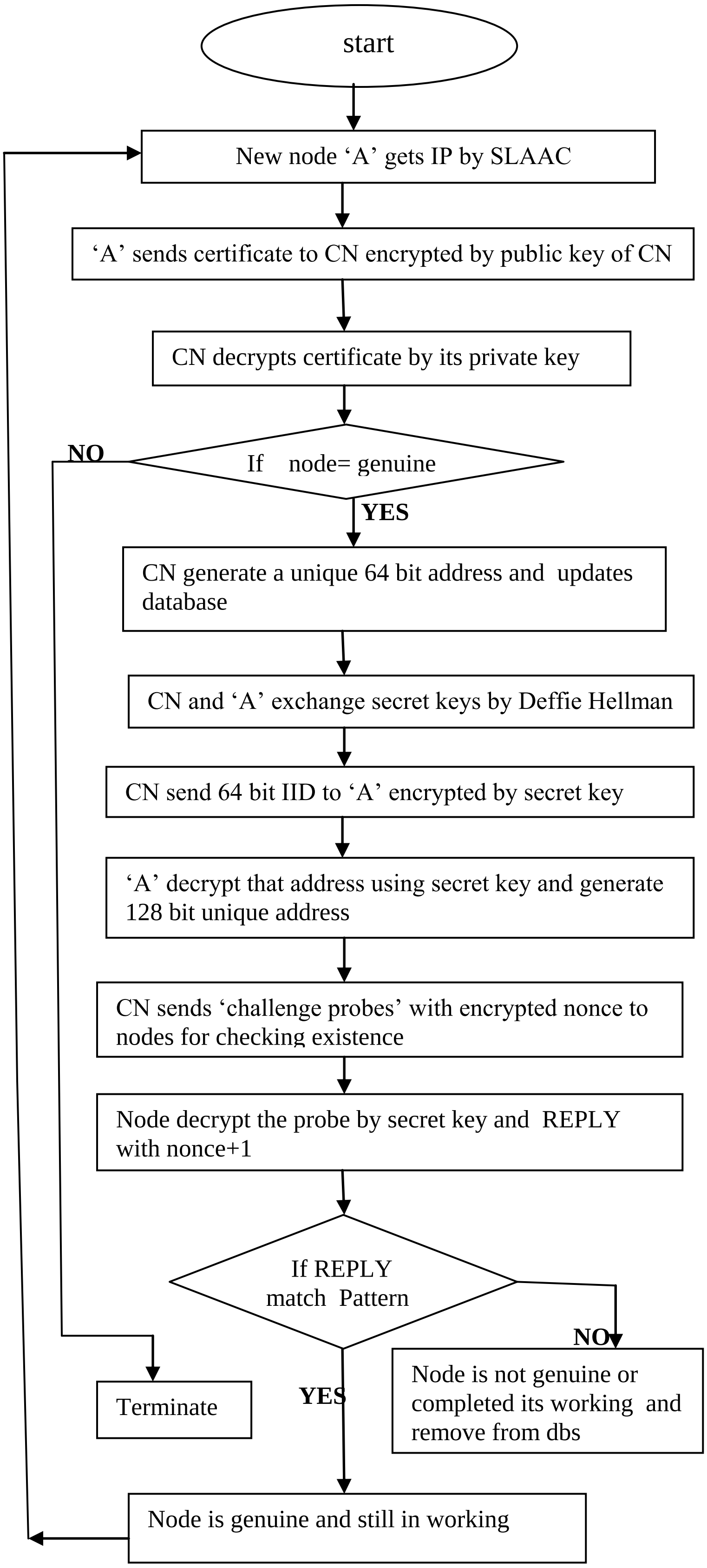
B. Diffie Hellman

In [DH76] Diffie and Hellman[14] describe a method for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms. Diffie-Hellman key agreement requires that both the sender and receiver of a message have key pairs. By combining one's private key and the other party's public key, both parties can compute the same shared secret number.This number can then be converted into cryptographic keying material. That keying material is typically used as a key-encryption key (KEK) to encrypt a content encryption key (CEK) which is in turn used to encrypt the message data.

C. Certificate authentication

A certificate is an electronic document that identifies an individual, a server, a company, or some other entity. A certificate also associates that identity with a public key. Certificate authorities, CAs, validate identities and issue certificates. CAs can be independent third parties or organizations that run their own certificate-issuing server software. The methods used to validate an identity vary depending on the policies of a given CA. A certificate issued by a CA binds a particular public key to the name of the entity the certificate identifies, such as the name of an employee or a server. n addition to a public key, a certificate always includes the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA.

D. Flow Chart


start
New node 'A' gets IP by SLAAC
'A' sends certificate to CN encrypted by public key of CN
CN decrypts certificate by its private key
If node= genuine
NO
YES
CN generate a unique 64 bit address and updates database
CN and 'A' exchange secret keys by Deffie Hellman
CN send 64 bit IID to 'A' encrypted by secret key
'A' decrypt that address using secret key and generate 128 bit unique address
CN sends 'challenge probes' with encrypted nonce to nodes for checking existence
Node decrypt the probe by secret key and REPLY with nonce+1
If REPLY match Pattern
NO
YES
Terminate
Node is not genuine or completed its working and remove from dbs
Node is genuine and still in working

7. Conclusion

As it is known that privacy is an important issue in present time because of number of attacks in the network. So the best method for securing a network is generating random interface identifier so that intruders can not track the IP address easily and data can be secured. Methods for generating random ID are CGA,Privacy Extension Method and SSAS. Here some techniques in which EUI-64,CGA and Privacy Extension has limitation and some are gud enough like SSAS and i-SeRP. SSAS takes less time to remove the vulnerabilities in comparison to CGA.But still SSAS has limitation because it takes a long computational time for processing. while i-SeRP calculate the risk value and then decide to use right model to counter the risks. In the proposed solution as 128 bit unique address is generated so it will prevent the malicious nodes to enter in the network and make the network secure. Because in the proposed work 'certification authentication' is used for preventing malicious node. And secrets will be exchanged by 'Diffie hellman Key Exchange Algorithm'. And to know the existence of malicious nodes, periodically challenges will be send.So it is more secure than other described method.

8. References

[1] Vineeth. M.V, Rejimoan.R, "Evaluating the performance of IPV6 with IPV4 and its distributed Security Policy",(ICT 2013).

[2] Ali ,W.N.A.W,et. Al Distributed policy for IPV6 deployment in sustainable energy & environment (ISESEE)2011.

[3] Durdagi E. and A. buldu IPV4/IPV6 security and threat comparison. Procedia- Social and Behavioral Science,2010.

[4] Chao, H. C.,sttuttgen, H.J.,wattington,D.G.,"IPV6: The Basics For The next generation Internet", IEEE communication Magazine,2004.

[5] Abdur Rahim chaudhary,"In-depth analysis of IPV6 security Postures",IEEE 2009.

[6] S.thomson,T. Narten,T. jinmei,"" IPV6 stateless Address Autoconfiguration", RFC 4862,Internet Engineering Task force,september 2007.

[7] Athirah Rosli,Wan Nor Ashiqin Wan Ali,Abidah Haji Mat Taib, "IPV6 Deployment: SecurityRisk assessment usin i-SeRP System in Enterprise Network" IEEE 2012.

[8] Steven J. and G. Peterson,threat modeling-Perhaps it's time. Security & Privacy,IEEE 2010.

[9] T. aura "Cryptographically Generated Addresses (CGA)", rfc 3972, Internet Engineering Task Force,march 2005.

[10] T. narten,R.draves, S.krishnan, "Privacy Extension for Stateless address Auto confihguration in IPV6",rfc 4941,2007.

[11] Hosnieh Rafiee ,Cristoph Meinel, "SSAS-A Simple Secure Addressing Scheme for IPV6 Autoconfiguration".

[12] http://tools.ietf.org/html/rfc4862

[13] http://tools.ietf.org/html/rfc4861

[14]https://www.ietf.org/rfc/rfc2631.txt

[15]]http://docs.oracle.com/cd/E19316-01/820-2765/6nebir7eb/index.html