A Survey on Domain Name System Security Approaches in IPv6

Bhargav Patel
PG Student
22/4, Amardeep Society, Navsari – 396445
India

ABSTRACT
The address pool for IPv4 has been exhausted. The internet service providers are using same addresses for addressing via subnettig. But it is not going to last forever. It is inevitable to use IPv6. In United States of America and Belgium, 33% and 98%, respectively of the whole network uses IPv6. So the security needs are increasing for IPv6. Now Domain Name System (DNS) is the most important part of Internet Protocol (IP). So it is must to secure the parameters of DNS. In the proposed study different approaches of DNS security for IPv6 network have been studied.

Keywords
Domain Name System (DNS), DNSSEC, SeND, CGA, TSIG

1. INTRODUCTION
Different machines which are connected over a network, is defined by Internet protocol which is a set of technical rules. Two versions IP version 6 (IPv6) and IP version 4 (IPv4) are available. The first version of Internet Protocol to be widely used is IPv4 and most of today's Internet traffic is handled by it. The available addresses are just over 4 billion which are not enough to last longer. IPv6 is a newer numbering system. A much larger address pool is provided by IPv6. It was deployed in 1999. The addressing needs should meet up to the requirements for IP addresses of clients in the whole world. The number of IP addresses available is the major difference between IPv4 and IPv6. With both of the versions, technical functioning of Internet remains the same. It seems that in future both versions will continue to operate well on the network simultaneously. Till date, support of both IPv4 and IPv6 addresses is available in most of the networks containing IPv6.

A stratified distributed naming system for computers, services or any resource connected to the web or a personal network is called as the domain name system (DNS). It associates different information with the domain names which are assigned to each of the participating entities. It translates domain names to the numerical IP addresses needed for locating devices and computer services worldwide. The functionality of the Internet depends on the domain name system.

It associates different information with the domain names which are assigned to each of the participating entities. It translates domain names to the numerical IP addresses needed for locating devices and computer services worldwide. The functionality of the Internet depends on the domain name system.

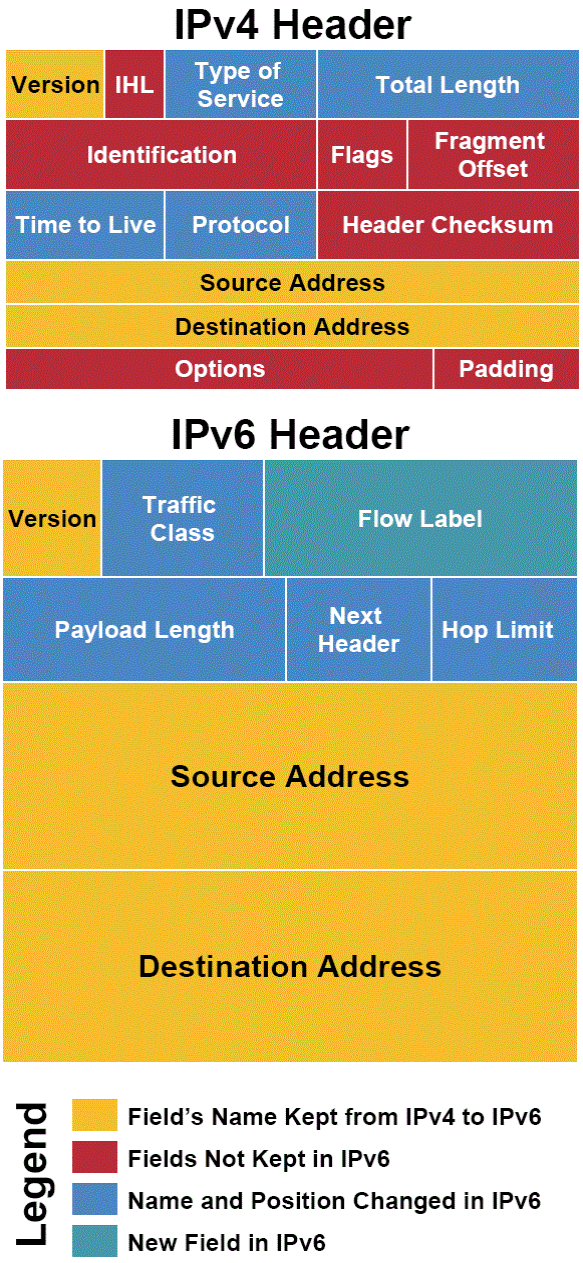

Figure 1: Comparison of IPv4 & IPv6 Header

2. DNS AND ITS FUNCTIONS

The Domain Name System (DNS) is a fundamental service of the Internet used by every application using IP addresses or IP devices. It is a distributed, hierarchical database which stores the mappings of IP addresses to hostnames. This hierarchy is referred to as the Domain Name System and is organized like an inverted tree starting from a single root.

A RR (Resource Record) is the basic data element that defines the structure and content of the domain name system. They are recognized by their type identifications. For example, type "AAAA"(Authentication, Authorization, Accounting and Auditing) (IPv6 address record) (RFC 3596) [1] is a RR that contains the IPv6 address of a host and type "NS" (Name Server record) is another RR used to identify the authoritative name servers for a zone. A zone is a portion of domain space that is authorized and administered by a primary name server and one or more secondary name servers.

When domain name of a web service is changed, it is important to update its domain name respective to their IP address into the RR. In IPv4 this process is known as Dynamic Domain Name System (DDNS) [2]. This protocol is both fast and secure for IPv4. But if IPv6 is considered, then it is not possible to use all the necessary protocols for IPv6 which are used for IPv4.

The DNS consists of a distributed tree structure of databases which contain individual records called Resource Records (RRs) - such as AAAA, PTR, etc. Each RR describes the characteristics of a zone (domain) and has a binary or wire-format, which is used in queries and responses and a text format used in zone files. There are two categories of name servers: Authoritative and Recursive [12].

- **Authoritative:** An authoritative name server is one that gives original and authoritative answers to DNS queries.
- **Recursive:** A recursive name server responds to queries concerning any domain. It initially checks its own records and cache for the solution to the question then, if it cannot notice any solution, it queries alternative servers before passing the response back to the creator of the query.

DNS update is the process of adding, changing or removing a RR record in a zone/domain's master file. Dynamic DNS (DDNS) (RFC 2136) [2] is a mechanism used to enable real-time, dynamic updates to entries in the DNS database. The clients or servers can automatically send updates to the authoritative name servers to modify the records they want to change.

3. SECURITY MECHANISMS

As the name suggests, Neighbor Discovery Protocol (NDP) (RFC 4861) [3] is used to find the appropriate node to forward the packets. But NDP was not much secured. That is why an extension to this protocol was suggested, which is called SEcure Neighbor Discovery (SEND) (RFC 3971) [4] protocol. SEND adds four new options to NDP messages. These options are as given below:

- Cryptographically Generated Address (CGA)
- Time Stamp
- Nonce
- Signature

These are the procedures required to forward the packet to appropriate destination. But it is also important to keep the DNS servers up-to-date when any change regarding domain name and IP address has been made. This process should be fast secure and simple.

3.1 DNS Security Extension (DNSSEC) [6]

DNSSEC verifies the authenticity and integrity of query results from a signed zone. It uses asymmetrical cryptography meaning that separate keys are used to encrypt and decrypt data to provide security for certain name servers with their respective administrative domains. When DNSSEC is used, all responses include a digital signature. This prevents DNS spoofing attacks because the attacker does not have the same private key as the server and thus will be unable to sign his own response and send it to the victim. Administrator of that zone needs to sign each domain and sub domain manually. Also, the zone private key should be stored offline. This is the reason that dynamic update cannot be fully supported. It cannot generate the signature, on-the-fly, in order to respond to real-time queries. Also, the use of DNSSEC cannot guarantee the data's confidentiality. Different algorithms are used to provide security in DNSSEC. It depends on the service provider to choose what kind of security is to provide to the customers. In the table given below different algorithm fields are shown which are used in DNSSEC.

Table 1: Different Algorithm for DNSSEC [RFC 6944] [7]

Field	Algorithm	RFCs	Implementations
1	RSA/MD5		DEPRECATED
3	DSA/SHA-1		OPTIONAL
5	RSA/SHA-1		REQUIRED
7	RSA/SHA1-NSEC3-SHA1	5155	RECOMMENDED
8	RSA/ SHA-256	5702	RECOMMENDED
10	RSA/ SHA-512		RECOMMENDED
12	GOST R 34.10-2001	5933	OPTIONAL
13	ECDSA/ SHA-256	6605	RECOMMENDED
14	ECDSA/ SHA-384		RECOMMENDED

3.2 Transaction Signature (TSIG) [8]

Endpoint authentication and data integrity using one-way hashing and shared secret keys is provided by TSIG to establish a trust relationship between two hosts which can be either two servers or a client and a server. The TSIG keys are manually exchanged between these two hosts and must be kept in a secure place. This protocol can be used to secure a dynamic update by verifying the signature with a cryptographic key shared with that of the receiver. The TSIG Resource Record (RR) has the same format as other records in a DDNS update request. Some fields contained in the TSIG

RR are: Name, Class, Type, Time to Live Resource Data (TTL RDATA), etc. The RDATA field is used to specify the type of algorithm used in a one-way hashing function along with the other information normally included.

This protocol is not suitable for servers which talk to many other servers for authentication. But it is suitable for many hosts which talk to few servers for resolving requests.

4. FLEXIBLE FRAMEWORK [13]

A modified and more flexible framework is required for DNS security in IPv6. This approach uses Cryptographically Generated Address (CGA) [5] protocol and Transaction Signature (TSIG) [8] protocol. The steps to generate modified TSIG are given below [10]:

4.1 Step 1: Retrieve the Public/Private Keys and Other Parameters from Cache

The key pairs are generated using a RSA algorithm or other CGA/SSAS (Cryptographically Generated Address/Simple Secure Addressing Scheme) [9] supported algorithms, during IP address generation using SeND. In this step all required CGA/SSAS parameters are obtained from cache. If the node cannot find these values in cache, it will generate key pairs using ECC or RSA algorithm.

4.2 Step 2: Encrypt the data using the DNS server's public key

DNS update message consists of a header, a zone, a prerequisite, an update and additional data. The header contains the control information (RFC 2136) [2]. The zone identifies the zones to which this update should be applied. The prerequisite prescribes the RRs that must be in the DNS database. The update contains the RR that needs to be modified or added. When modified framework is used, the update and prerequisite sections should be encrypted using the DNS server's public key and should not be sent unencrypted. The additional data is that data which is not a part of the DNS update, but is necessary in order to process this update. The node first encrypts the prerequisite data and the update section containing RRs separately using the DNS server's public key and the same algorithm that the DNS server uses for its key pair generation, which can be RSA, ECC [11] or any other future algorithm. Then it places them in the update and prerequisite sections of the DNS message. To improve this, it is possible to encrypt the update and prerequisite sections using a symmetric algorithm and encrypt the shared secret using the DNS server's public key. In this case the overhead for using public/private key encryption will be mitigated.

4.3 Step 3: Generate the Signature

To generate the signature, all CGA parameters (modifier, collision count and subnet prefix excluding the public key) that were concatenated with the encrypted DNS update message (such as the prerequisite and the update sections) and the Time Signed field, are signed using an ECC algorithm and the private key which was generated in the initial step for the IP address generation. This signature can be added, as an option, to the Other Data section of TSIG RDATA field. The data format of the signature is shown figure 3 [10]. In RDATA the timestamp is same as the time signed. This approach will prevent replay attacks by changing the content of the signature each time a node wants to send a DNS Update Request. Other Data section is added in TSIG RDATA field to accommodate the addition of a signature and public keys. Figure 4 shows options to the TSIG RDATA field [10].

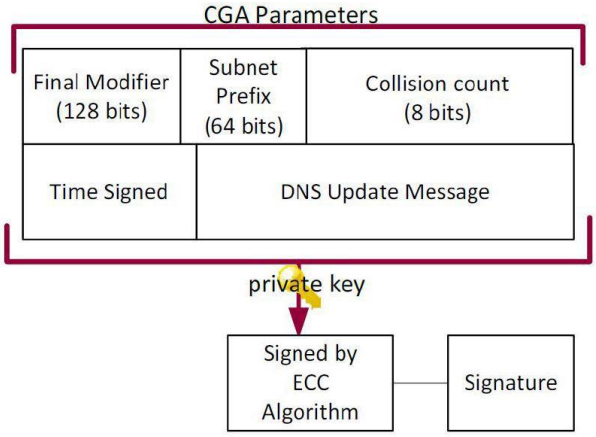

Figure 2: Modified TSIG Signature Content

Source: RFC 2845 (2013) [13]

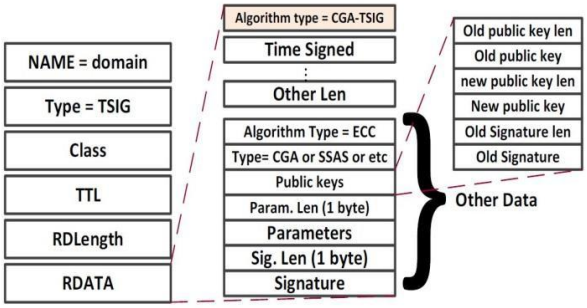

Figure 3: Modified TSIG RR Format

Source: RFC 2845 (2013) [13]

Other Len defines the overall length of the Other Data which contains the algorithm type used to generate key pairs and sign the message which, by default, would be ECC. The algorithm which is used by SeND is indicated by the Type. This field is reserved for the use of future algorithms in place of CGA. The assigned default value for CGA is 1. Other algorithms would be assigned numerical values sequentially. For example, SSAS could be assigned a value of 2. If the node does not use SeND and it generates its public/private key by itself with no association to its IP address then this value will be set to 0.

This modified Transaction Signature (TSIG) must be verified also. The steps of TSIG verification are as followed:

- Process the CGA/SSAS verification
- Check Time Signed
- Verify the Signature
- Verify the Public Key

5. CONCLUSION

In this paper, we have studied different protocols for the security of Domain Name System (DNS) Resource Record (RR) update. The study shows that different protocols like DNSSEC, TSIG, SEND, etc. are sufficient to provide security in IPv4 network. But they fail at proving security to IPv6. The modified TSIG-CGA algorithm covers most possible aspects of security in IPv6 network for DNS. This modified approach is sustainable against attacks like IP spoofing, DNS Dynamic Update Spoofing, Resolver Configuration Attack, Replay Attack, etc. The improvement of TSIG protocol is ongoing. It

still has to be improvised to be used in the actual network for practical application.

6. REFERENCES

[1] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003, http://www.rfc-editor.org/info/rfc3596

[2] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997, http://www.rfceditor.org/info/rfc2136

[3] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007

[4] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005, http://www.rfc-editor.org/info/rfc3971

[5] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005, http://www.rfc-editor.org/info/rfc3972

[6] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000, http://www.rfc-editor.org/info/rfc3007

[7] Rose, S., "Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status", RFC 6944, April 2013, http://www.rfc-editor.org/info/rfc6944

[8] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000, http://www.rfc-editor.org/info/rfc2845

[9] H. Rafiee, C. Meinel, "A Simple Secure Addressing Scheme for IPv6 AutoConfiguration", IEEE, the 11th Annual Conference on Privacy, Security and Trust, July 2013

[10] Rafiee, H.; Meinel, C., "A Secure, Flexible Framework for DNS Authentication in IPv6 Autoconfiguration," Network Computing and Applications (NCA), 2013 12th IEEE International Symposium on , vol., no., pp.165,172, 22-24 Aug. 2013

[11] D. L. R. Brown, "SEC 1: Elliptic Curve Cryptography", Certicom Research, http://www.secg.org/download/aid-80/sec1-v2.pdf, 2009

[12] What Is the Difference between Authoritative and Recursive DNS Nameservers? http://blog.opendns.com/2014/07/16/difference-authoritative-recursive-dns-nameservers/

[13] H. Rafiee, M. V. Loweis, C. Meinel, Hasso Plattner Institute, "Transaction SIGnature (TSIG) using CGA Algorithm in IPv6", INTERNET-DRAFT for RFC 2845, July 2013, http://tools.ietf.org/id/draft-rafiee-intarea-cga-tsig-03.tx