www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1351-1354

Security and Key Distribution in Binding of Ip to Dns

Arvind Kumar Gupta* ,Pravin Tripathi,Satypal
B.Tech.(IT)
Institute of Technology and Mangement
Gida ,Gorakhpur U.P.
*guptaak06@gmail.com
pravin4524@gmail.com
satypal@hotmail.com

Abstract:

The mapping or binding of IP addresses to host names became a major problem in the rapidly growing Internet and the higher level binding effort went through different stages of development up to the currentlyusedDomain Name System (DNS) The DNS Security is designed to provide security by combining the concept of both the Digital Signature and Asymmetric key (Public key) Cryptography. Here the Public key is send instead of Private key. The DNS security uses Message Digest Algorithm to compress the Message(text file) and PRNG(Pseudo Random Number Generator) Algorithm for generating Public and Private key. The message combines with the Private key to form a Signature using DSA Algorithm, which is send along with the Public key.

The receiver uses the Public key and DSA Algorithm to form a Signature. If this Signature matches with the Signature of the message received, the message is Decrypted and read else discarded.

Keywords: Digital Signature,PRNG(Pseudo Random Number Generator), Asymmetric key cryptography, DSA, Public key, Private key.

1 INTRODUCTION

The Domain Name System(DNS) has become a critical operational part of the Internet Infrastructure, yet it has no strong security mechanisms to assure Data Integrity or Authentication. Extensions to the DNS are described that provide these services to security aware resolves are applications through the use of Cryptographic Digital Signatures. These Digital Signatures are included zones as resource records.

The extensions also provide for the storage of Authenticated Public keys in the DNS. This storage of keys can support general Public key distribution services as well as DNS security. These stored keys enables security aware resolvers to learn the authenticating key of zones, in addition to those for which they are initially configured. Keys associated with DNS names can be retrieved to support other protocols. In addition, the security extensions provide for the Authentication of DNS protocol transactions.

1.1 Fundamental of DNS

The DNS not only supports host name to network address resolution, known as forward resolution, but it also supports network address to host name resolution, known as inverse resolution. Due to its ability to map human memorable system names into computer network numerical addresses, its distributed nature, and its robustness, the DNS has evolved into a critical component of the Internet. Without it, the only way to reach other

computers on the Internet is to use the numerical network address.

1.2 Domain Name Space

The DNS is a hierarchical tree structure whose root node is known as the root domain. A label in a DNS name directly corresponds with a node in the DNS tree structure. A label is an alphanumeric string that uniquely identifies that node from its brothers. Labels are connected together with a dot notation, ".", and a DNS name containing multiple labels represents its path along the tree to the root. Labels are written from left to right. Only one zero length label is allowed and is reserved for the root of the tree.

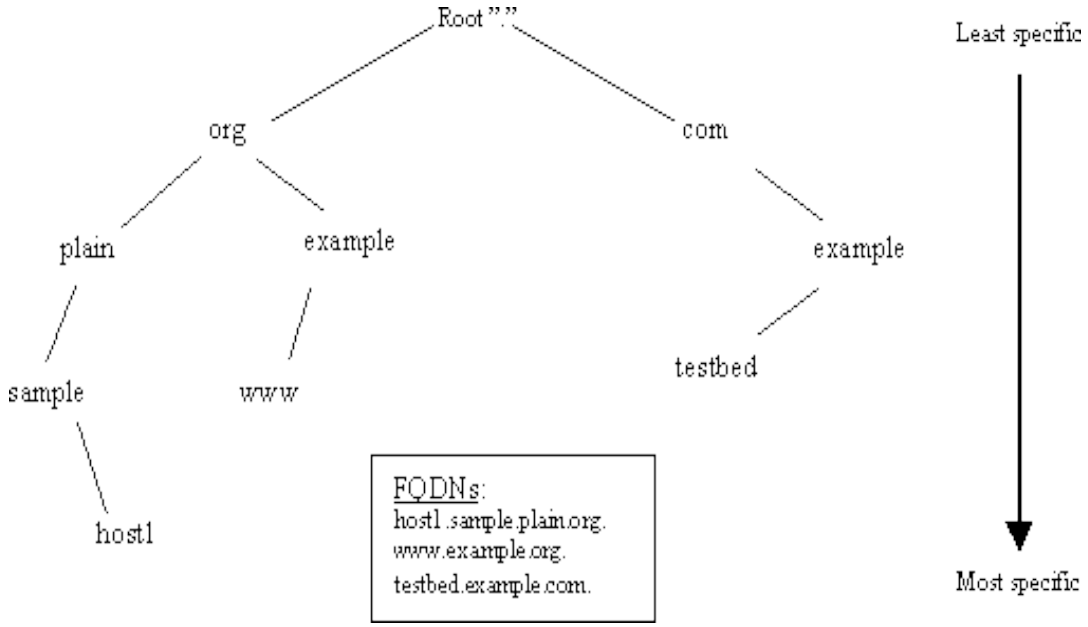

Figure 1 tree structure of DNS

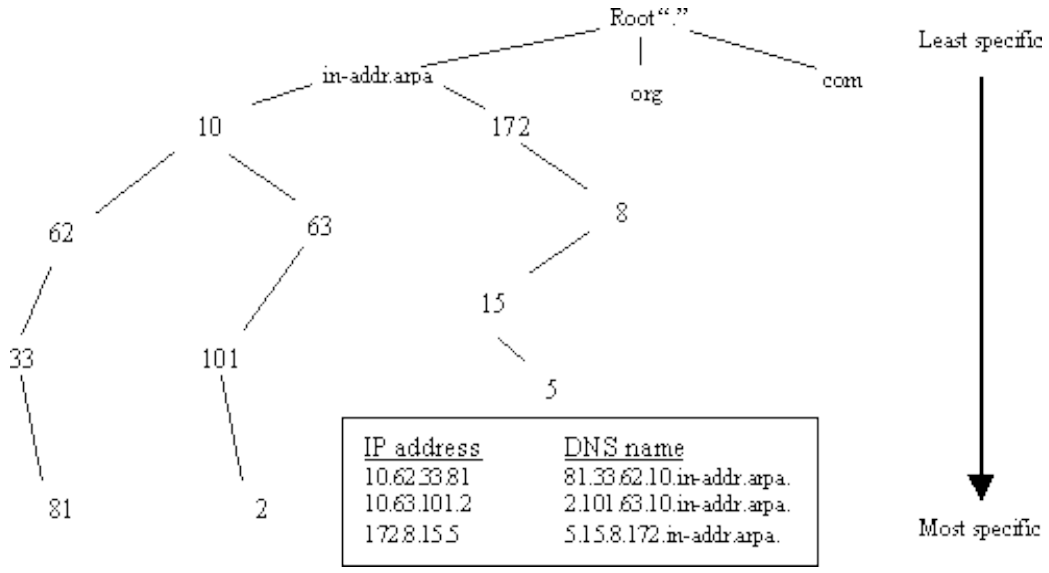

Figure2-Example of inverse domain and domain name space

2. DNS Component

The DNS has three major components, the database, the server, and the client.]. The database is a distributed database and is comprised of the Domain Name Space, which is essentially the DNS tree, and the Resource Records (RRs) that define the domain names within the Domain Name Space. The server is commonly referred to as a name server. Name servers are typically responsible for managing some portion of the Domain Name Space and for assisting clients in finding information within the DNS tree. Name servers are authoritative for the domains in which they are responsible. They can also serve as a delegation point to identify other name servers that have authority over subdomains within a given domain.

The RR data found on the name server that makes up a domain is commonly referred to as zone information. Thus, name servers have zones of authority. A single zone can either be a forward zone (i.e., zone information that pertains to a given domain) or an inverse zone (i.e., zone information that maps IP addresses into DNS host names). DNS allows more than one name server per zone, but only one name server can be the primary server for the zone. Primary servers are where the actual changes to the data for a zone take place. All the other name servers for a zone basically maintain copies of the primary server's database for the zone. These servers are commonly referred to as secondary servers

2.1 DNS transaction

DNS transactions occur continuously across the Internet. The two most common transactions are DNS zone transfers and DNS queries/responses. A DNS zone transfer occurs when the secondary server updates its copy of a zone for which it is authoritative. The secondary server makes use of information it has on the zone, namely the serial number, and checks to see if the primary server has a more recent version. If it does, the secondary server retrieves a new copy of the zone. A DNS query is answered by a DNS response. Resolvers use a finite list of name servers, usually not more than three, to determine where to send queries. If the first name server in the list is available to answer the query, than the others in the list are never consulted. If it is unavailable, each name server in the list is consulted until one is found that can return an answer to the query. The name server that receives a query from a client can act on behalf of the client to resolve the query. Then the name server can query other name servers one at a time, with each server consulted being presumably closer to the answer. The name server that has the answer sends a response back to the original name server, which then can cache the response and send the answer back to the client. Once an answer is cached, a DNS server can use the cached information when responding to subsequent queries for the same DNS information. Caching makes the DNS more efficient, especially when under heavy load. This efficiency gain has its tradeoffs; the most notable is in security.

3. KEYs in Domain Name System

The Domain Name System (DNS) is the global hierarchical replicated distributed database system for Internet addressing, mail proxy, and other information. The DNS has been extended to include digital signatures and cryptographic keys. Thus the DNS can now be secured and used for secure key distribution.

The SHA1 Secure Hash Algorithm which produces a larger hash, has been developed. By now there has been sufficient experience with SHA1 that it is generally acknowledged to be stronger than MD5. While this stronger hash is probably not needed today in most secure DNS zones, critical zones such a root, most top level domains, and some second and third level domains, are sufficiently valuable targets that it would be negligent not to provide what are generally agreed to be stronger mechanisms.

Furthermore, future advances in cryptanalysis and/or computer speeds may require a stronger hash everywhere. In addition, the additional computation required by SHA1 above that required by MD5 is insignificant compared with the computational effort required by the RSA modular exponentiation.

3.1 RSA Public KEY Resource Records

RSA public keys are stored in the DNS as KEY RRs using algorithm number. The structure of the

algorithm specific portion of the RDATA part of such RRs is as shown below.

Field	Size
exponent length	1 or 3 octets (see text)
exponent	as specified by length field
modulus	remaining space

For interoperability, the exponent and modulus are each limited to 4096 bits in length. The public key exponent is a variable length unsigned integer. Its length in octets is represented as one octet if it is in the range of 1 to 255 and by a zero octet followed by a two octet unsigned length if it is longer than 255 bytes. The public key modulus field is a multiprecision unsigned integer. The length of the modulus can be determined from the RDLENGTH and the preceding

RDATA fields including the exponent. Leading zero octets are prohibited in the exponent and modulus.

3.2 RSA/SHA1 SIG Resource Records

RSA/SHA1 signatures are stored in the DNS using SIG resource records (RRs) with algorithm number 5. The signature portion of the SIG RR RDATA area, when using the RSA/SHA1 algorithm, is calculated as shown below. The data signed is determined as specified in RFC 2535. See RFC 2535 for fields in the SIG RR RDATA which precede the signature itself.

hash = SHA1 (data)

signature = (01 | FF* | 00 | prefix | hash) ** e (mod n)

Where SHA1 is the message digest algorithm documented in [FIP180],"|" is concatenation, "e" is the private key exponent of the signer, and "n" 7. ’.

is the modulus of the signer’s public key. 01, FF, and 00are fixed octets of the corresponding hexadecimal value. "prefix" isthe ASN.1 BER SHA1 algorithm designator prefix required in PKCS1 that is,

hex 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14

This prefix is included to make it easier to use standard cryptographic libraries. The FF octet MUST be repeated the maximum number of times such that the value of the quantity being exponentiated is one octet shorter than the value of n.

4.Performance Considerations

General signature generation speeds are roughly the same for RSA and DSA . With sufficient pre-computation, signature generation with DSA is faster than RSA. Key generation is also faster for DSA. However, signature verification is an order of magnitude slower with DSA when the RSA public exponent is chosen to be small as is recommended for KEY RRs used in domain name system (DNS) data authentication.

5. REFERENCES

1. Albitz, P. and Liu, C., (1997) ‘DNS and Bind’, 2nd Ed., Sebastopol, CA, O’Reilly & Associates, pp.1-9.
2. IETF DNSSEC WG, (1994) ‘DNS Security (dnssec) Charter’, IETF
3. Michael Foley and Mark McCulley, Edition(2002) ‘JFC Unleashed’ Prentice –Hall India.
4. Mockapetris, P., (1987) ‘Domain Names - Concepts and Facilities’.
5. RFC 4033 ‘DNS security and requirement’.
6. RFC 3110, ‘SIGNs and RSA KEYs in Domain name system