Analysis of Security Systems for DNS using Cryptography

Sona V
Lecturer in Computer Engineering, Swami Nithyananda Polytechnic College, Kasaragod, Kerala, India

ABSTRACT

A major issue in the quickly expanding Internet was the mapping or binding of IP addresses to host names, and the higher level binding effort went through various stages of development before the current Domain Name System (DNS) was developed (DNS). Digital signatures and asymmetric key cryptography (public key) are combined in DNS Security to ensure security. Private keys aren't sent in this case, but the public key is instead. There are two algorithms used in DNS security: Message Digest Algorithm and PRNG (Pseudo Random Number Generator) Algorithm. DSA Algorithm is used to create a Signature from the message and the private key, which is then sent with the public key.

Keywords*: DNS, Digital Signature, Cryptography, ECC, ECDSA, security systems, cryptography, DNSSEC, DNS Security, DNS Transaction*

Introduction

Despite the fact that it lacks a safe mechanism to ensure data integration or verification, Internet communications are widely used. Application developers who are concerned about security will appreciate the services provided by DNS extensions, which store valid public keys as resource entries in the DNS and support both generic public key distribution services and DNS security. Resolvers that are security-aware can access the zone's authenticating key using the saved keys, and these keys can also be used to maintain other protocols and extensions.

DNS Security combines the concepts of digital signatures and asymmetric key (public key) **cryptography** to guarantee security. Instead of sending the private key, the public key is sent here. The goal of this project is to use cryptography to create a DNS security solution. The Message Digest Algorithm and the PRNG Algorithm (Pseudo Random Number Generator) are used by DNS security to compress messages and generate public and private keys, respectively.

The hosts.txt file's scalability issues can be solved using the DNS as an Internet standard. Since then, the DNS has become an essential part of the Internet due to its extensive use and its ability to quickly and fairly reliably translate host names into IP addresses for both users and applications.

Stanford Research Institute's Network Information Center (SRI-NIC), the Internet's primary authority for unique host names, took over the responsibility. A single file called hosts.txt was kept by the SRI-NIC that sites would constantly update with their host name to IP address mappings. As the Internet evolved, managing files became more complicated, and hostnames had to be unique throughout the entire internet. As the internet's size grew, it became hard to guarantee that each host name would be unique. There was a need for a network protocol that could be used worldwide because of the necessity for hierarchical name structure and distributed management of host names. [ALIU]. [1]

Fundamentals of DNS

In addition to forward resolution, which is the process of resolving a host name to a network address, inverse resolution is also supported by the DNS. The DNS has evolved into a crucial part of the Internet because of its capacity to map human memorable system names into computer network numerical addresses, its distributed nature, and its robustness. Only by using the numerical network address can a computer's location on the Internet be determined without this protocol. The DNS is highly depended upon to acquire an IP address by simply referencing a computer system's Fully Qualified Domain Name because using IP addresses to connect to faraway computer systems is not an ideal representation of a system's location on the Internet (FQDN). Basically, a FQDN is a DNS host name that tells the DNS server where to find this host name. [2]

Domain Name Space

The Domain Name System (DNS) is a tree-like structure. There is a node at the top of the tree that is called the root domain. Named nodes in the DNS tree have corresponding labels in DNS names. An alphanumeric string known as a label is used to distinguish one node from its neighbours. Connecting labels is done with dots ("."), and labels are written from left to right. One way to see the journey a DNS name takes to the root of the tree is to use labels. The root of the tree can only have one zero-length label. The root zone is the technical term for this area. Due to the root label's zero length [RFC 1034], all FQDNs finish in a dot.

DNS Components

The database, the server, and the client make up the DNS. [RFC 1034]. Distributed databases include the Domain Name Space (DNS) and Resource Records (RRs), which specify the domain names within the Domain Name Space. The server is commonly referred to as a name server and is usually in charge of arranging a piece of the Domain Name Space as well as assisting clients in locating data inside the DNS tree. For the domains for which they are accountable, name servers act as the final arbiter of truth. These name servers are used to identify additional name servers that control subdomains inside a specific domain.

DNS Transactions

All around the Internet, DNS transactions are always taking place. DNS zone transfers and DNS queries/responses are the two most typical types of transactions in the industry. An authoritative DNS zone transfer occurs when a secondary server updates its copy of a zone for which it holds the copyright. In order to determine if the primary server has a more recent version, the secondary server uses the zone information it has, specifically the serial number. If it does, a fresh copy of the zone is downloaded to the backup server.

DNSSEC

This working group was established in 1994 by the IETF in order to address the security concerns around the DNS protocol. DNSSEC extensions are the common name given to these add-ons. The protocol's security features are intended to work with DNS implementations that don't pay attention to security issues. Because it was purposefully designed to be extendable, the RR component in the DNS was used by the IETF. For DNS zones that want to use DNSSEC, the WG created a new set of RRs to store the security information. Existing Resource Records can be combined with new RR kinds. In this way, DNSSEC-protected zones' DNS security information can be accessed by servers that aren't security-aware.

DNS Security

There is no way for DNS to tell if the domain name data is authentic or if it has been falsified, as it was originally built. DNS cache poisoning and DNS spoofing are two examples of attacks made possible by this security flaw. This can be done by anticipating a DNS message ID and responding before the legitimate DNS server due to the lack of strong authentication between the servers exchanging updates. When a DNS server is hacked, it will make a request to an attacker's DNS server, which will return the erroneous host to IP mapping.

An IETF standard known as DNSSEC (DNS Security Extensions) was established to solve DNS vulnerabilities and guard against online attacks. By identifying and solving DNS security flaws, DNSSEC aims to improve the overall security of the Internet. According to DNSSEC implementation, the system is made more secure by adding an authentication capability to DNS. [3]

Review of Literature

As a successor for the "host table" system, the DNS was created. Names for network resources at a higher abstract level than network (IP) addresses were meant to be provided by the two systems (see, e.g.,[**RFC625**], [**RFC811**], [**RFC819**], [**RFC830**], [**RFC882**]). Recently, DNS has become a convenient database for the Internet, with several proposals for new capabilities. So yet, just a few of these ideas have been adopted and implemented into actual programmes. DNS usage is frequently driven solely by the fact that it already exists and is widely deployed, rather than by the fact that its structure, capabilities, and content are optimal for the particular data application at hand. The history of the DNS is examined in this document, as well as some of the newer applications. The overloaded process is thus said to be ineffective in many cases. Rather, it argues that the DNS should be complemented with systems that are more suited to the intended purposes and provides a conceptual framework and reasoning for one such system. To establish an IP connection, the host making the connection must know the distant system's IP address beforehand. In a network, a 32-bit IP address identifies where a computer or device is located. Typically, each octet of a 32-bit address is represented by a decimal number. A dot character separates the four decimal numbers from each other ("."). There is a practical limit to how many IP addresses a human can remember without the aid of some form of directory assistance, even if four decimal numbers are simpler to remember than thirty-two 1‟s and 0‟s. The directory is just a list of IP addresses and their associated host names. Stanford Research Institute's (SRI) Network Information Center (SRI-NIC) became the Internet's primary authority for ensuring that each host name was unique. A single file called hosts.txt was kept by the SRI-NIC that sites would constantly update with their host name to IP address mappings. The difficulty was that as the Internet grew, so did the file, making it more and more difficult to maintain. As a further requirement, the host names had to be unique on the Internet at large. It became increasingly difficult to ensure the uniqueness of a host name as the Internet grew in size. New networking protocols that may be used globally were made possible by the demand for features such as hierarchical names and distributed administration of host names [ALIU]. [4-7]

Objective:

Using asymmetric (public key) cryptography in conjunction with digital signatures to ensure that data by transmitting the public key via a network.

Research Methodology:

This research relies on data that has already been published in the form of published articles and papers. The information used to prepare this report was culled from a variety of reliable online sources.

Result and Discussion:

Attacks on the Internet have repeatedly taken advantage of DNS flaws. By manipulating DNS records, an attacker can easily "deface" a web server and redirect its domain name to a server under their control. End-to-end authenticity and data integrity are provided using transaction and zone signing signatures in DNSSEC. Clients and servers both compute transaction signatures as requests and replies are sent back and forth between them. As long as both parties have a secret key, they can use DNSSEC to authenticate and authorise each other's DNS communications by using the message authentication code (MAC). A damaged server functioning as a resolver is not protected by transaction signatures since they guarantee integrity only if a client engages in a transaction with the server that is authoritative for the returned data. Zone signing requires the use of a zone key, which is a public key for a digital signature technique. An additional SIG resource record is added to every resource record in the DNS database that contains a digital signature computed over the resource record. 1 Because the signature is created by the entity that owns the zone, zone signing also protects data that has been conveyed. [8]

Key Generation

Careful key generation is sometimes underestimated but extremely crucial in any cryptographically safe system. If an adversary can guess sufficiently to minimise the size of the likely key space so that it can be thoroughly searched, the strongest algorithms employed with the longest keys are of no value. RFC 4086 [14] provides technical guidance on how to generate random keys. The random number generator used for key generation should be checked to see if it corresponds to these guidelines. These keys are especially vulnerable since they are more valued as a target and can be attacked for longer periods of time than keys with a limited effective period. Long-term key generation should take place off-line, preferably via an air gap or at the at least, high-level secure hardware, and should be isolated from the network. Creating and verifying signature, encryption and decryption. [9,10]

A Domain Name System is depicted in Fig 1. A DNS name is represented by each node in the DNS tree. DNS domains, machines, and services are only a few instances of what DNS names can be. [11]

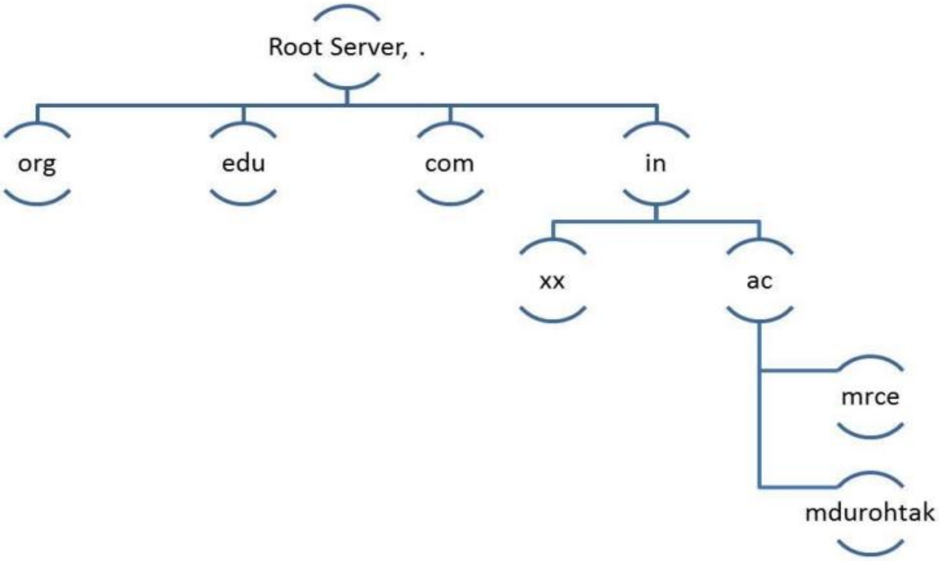
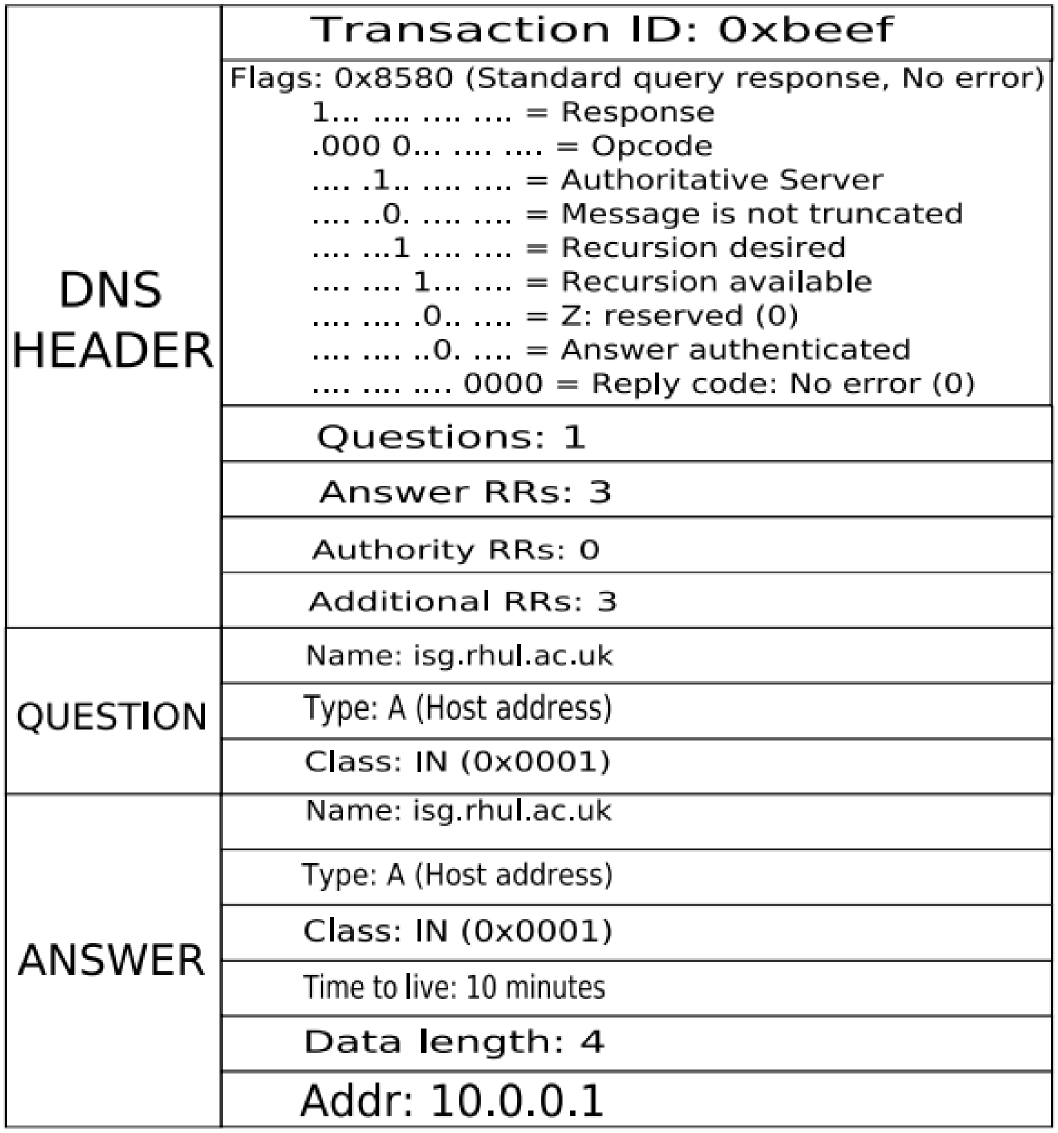


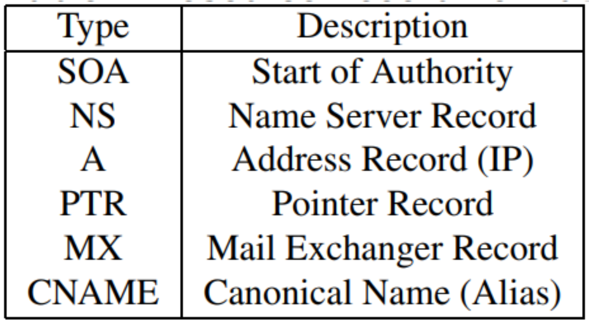
Fig. 1 Domain Name System

Figure 2 illustrates the format of DNS queries and responses. DNS queries are shown in full, with each question and answer displayed.



DNS HEADER	Transaction ID: 0xbeef
	Flags: 0x8580 (Standard query response, No error) 1... .... = Response .000 0... .... = Opcode .... .1.. .... = Authoritative Server .... ..0. .... = Message is not truncated ....1 .... = Recursion desired .... 1... .... = Recursion available .... .0.. .... = Z: reserved (0) ....0. .... = Answer authenticated .... 0000 = Reply code: No error (0)
	Questions: 1
	Answer RRs: 3
	Authority RRs: 0
	Additional RRs: 3
QUESTION	Name: isg.rhul.ac.uk
	Type: A (Host address)
	Class: IN (0x0001)
ANSWER	Name: isg.rhul.ac.uk
	Type: A (Host address)
	Class: IN (0x0001)
	Time to live: 10 minutes
	Data length: 4
	Addr: 10.0.0.1

Table 1 Resource Record Format



Type	Description
SOA	Start of Authority
NS	Name Server Record
A	Address Record (IP)
PTR	Pointer Record
MX	Mail Exchanger Record
CNAME	Canonical Name (Alias)

The RR is referenced by the domain name. For a cached RR, the Time To Live (TTL) is the amount of time it can be regarded valid. RRs are often classified as IN (Internet) networks, which is a subset of the IN class. Table 1 lists the most frequently used Type values. [12-14]

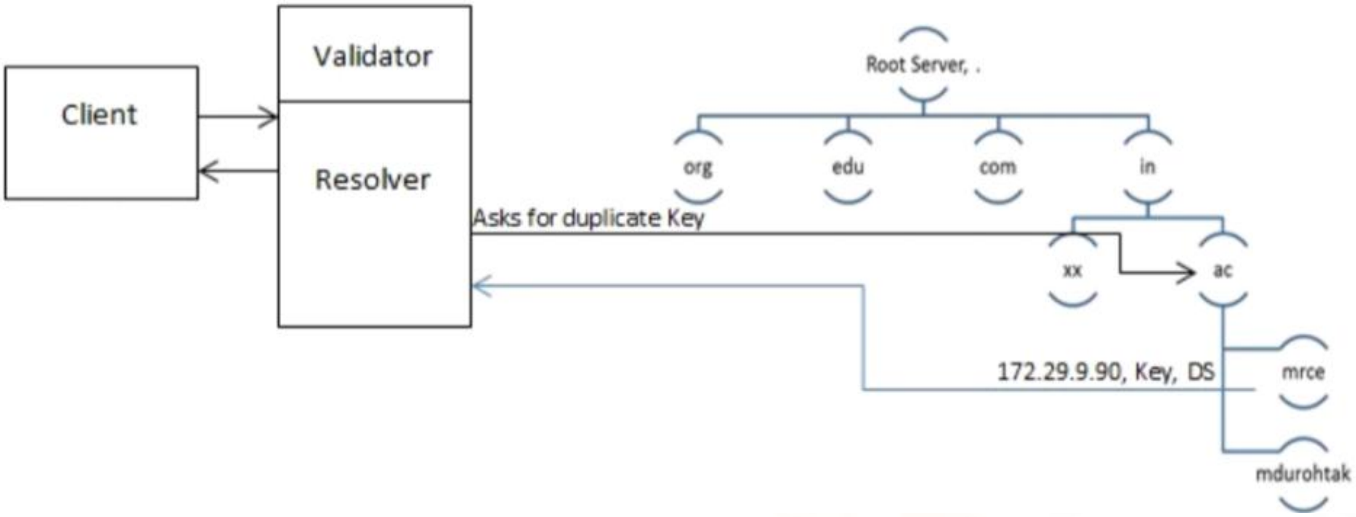


Fig. 2 Basic Idea of Security

Key and DS (Digital Signature) are sent together with the response. As a last step, a resolver requests a duplicate key from the top-level domain. After that, the validator determines if the two keys are same. If the answer is affirmative, then the data is safe. It also verifies the authenticity of the DS. [15] The info is authentic if it is accurate. Finally, the data is checked and sent back to the client following the same approach for each of the above domains.

Conclusion

The DNS as an Internet standard to tackle the challenges of scalability surrounding the hosts.txt file. Since then, the widespread use of the DNS and its capacity to resolve host names into IP addresses for both users and applications alike in a timely and fairly reliable manner, makes it a crucial component of the Internet. The distributed management of the DNS and support for redundancy of DNS zones across different servers supports its robust properties. However, the original DNS protocol standards did not contain security. Without security, the DNS is subject to attacks ranging from cache poisoning techniques, client flooding, dynamic update vulnerabilities, information leakage, and compromise of a DNS server‟s authoritative files.

References

[1] Albitz, P. and Liu, C., (1997) „DNS and Bind‟, 2nd Ed., Sebastopol, CA, O‟Reilly &Associates, pp.1-9.

[2] HerbertSchildt, Edition (2003) „The Complete Reference JAVA 2‟ Tata McGraw Hill Publications

[3] IETF DNSSEC WG, (1994) „DNS Security (dnssec) Charter‟, IETF.

[4] Michael Foley and Mark McCulley, Edition(2002) 'JFC Unleashed‟

Prentice-Hall India.

[5] Mockapetris, P., (1987) „Domain Names - Concepts and Facilities‟.

[6] A.Sakthivel, R. Nedunchezhian, Improved The Execution Speed of Ecdsa Over Gf(2 n) Algorithm for Concurrent Computation Journal of Theoretical and Applied Information Technology, (2013).

[7] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, Elliptic Curve Cryptography, ACM Ubiquity, 9(20) (2008).

[8] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, Elliptic Curve Cryptography, ACM Ubiquity, 9(20) (2008).

[9] Ravi Kishore Kodali, “Implementation of ECDSA in WSN”, International Conference on Control Communication and Computing (ICCC), IEEE, 2013.

[10] Shweta Lamba, Monika Sharma, “An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA)”, International Conference on Machine Intelligence Research and Advancement, IEEE, 2013.

[11] Aqeel Khalique Kuldip Singh Sandeep Sood, “Implementation of Elliptic Curve Digital Signature Algorithm”, International Journal of Computer Applications (0975 – 8887), Volume 2 – No.2, May 2010.

[12] Neetesh Saxena, Narendra S. Chaudhari, “Secure Encryption with Digital Signature Approach for Short Message Service”, IEEE, 2012.

[13] Weiler and J. Ihren. Minimally covering NSEC records and DNSSEC on-line signing. RFC 4070, Internet Engineering Task Force, Apr. 2006.

[14] D. Wessels and M. Fomenkov. Wow, that’s a lot of packets. Technical report, Cooperative Association for Internet Data Analysis — CAIDA, San Diego Supercomputer Center, University of California, San Diego, 2003.

[15] Aqeel Khalique Kuldip Singh Sandeep Sood, “Implementation of Elliptic Curve Digital SignatureAlgorithm”, International Journal of Computer Applications (0975 – 8887), Volume 2 – No.2, May 2010.