GALGOTIAS UNIVERSITY
(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

SECURITY SYSTEM FOR DNS USING CRYPTOGRAPHY

A Project Report of Capstone Project - 2

Submitted by

AKASH

(1613114007 / 16SCSE114042)

in partial fulfillment for the award of the degree

of

Bachelor of Technology

IN

Computer Science and Engineering

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

Under the Supervision of

Dr. SUDEEPT SINGH YADAV
M.Tech., Ph.D, Professor

APRIL / MAY- 2020

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that project report " SECURITY SYSTEM FOR DNS USING CRYPTOGRAPHY" is the bonafide work of AKASH (1613114007)" who carried out the project work under my supervision.

SIGNATURE OF HEAD

Dr. MUNISH SHABARWAL,
PhD (Management), PhD (CS)
Professor & Dean,
School of Computing Science & Engineering

SIGNATURE OF SUPERVISOR

Dr. SANJEEV KUMAR PIPAL,
M.Tech., Ph.D.,
Professor
School of Computing Science & Engineering

TABLE OF CONTENTS

- Abstract
- Introduction
    - ❖ Overall description
    - ❖ Purpose
    - ❖ Motivations and scope
- Proposed model
- Existing System
- Implementation or Architecture Diagrams
- Output/Results
- Conclusion
- References

[1]. ABSTRACT

Domain Name System is a protocol that resolves hostnames to IP Addresses over the Internet. DNS, being an open source, it is less secure and it has no means of determining whether domain name data comes from an authorized domain owner. So, these vulnerabilities lead to a number of attacks, such as, cache poisoning, cache spoofing etc. Hence, there is a needofsecuringDNS.DigitalSignaturesareagoodway of authenticating the domain owners. This paper presents the Domain Name System security concept, Digital Signature algorithms helps in providinggood level of security to DNS. It involves the signing of DNS using cryptographical algorithms (e.g., RSA, DSA etc.)

The Mapping of IP address to hostname become a significant issue in the quickly developing web what's more, more significant level finding a fore experienced various phases of advancement of the nation use space name framework security is intended to give security by consolidating the idea off the vessel the advanced signature and uneven key open key cryptography open please send of private key that you realize security utilizes a message digest calculation to pack the message furthermore, prng pseudo arbitrary number generator calculation for creating open and private key the message joins the private key to frame a mark using DFS calculation which is sent along with the open key the collector utilizes the open DSLR the previous mark this mark matches with the mark of the messages if the message is unscrambled and retails disposed of. To contact someone else on the Internet we need to type a location into our PC - a name or a number. That address must be one of a kind so PCs realize where to locate one another. ICANN organizes these interesting identifiers over the world. Without that coordination we wouldn't have one worldwide Internet. When composing a name, that name

must be first converted into a number by a framework before the association can be set up. That framework is known as the Domain Name System (DNS) and it makes an interpretation of names like www.icann.org into the numbers – called Internet Protocol (IP) addresses. ICANN organizes the tending to framework to guarantee all the addresses are one of a kind. As of late vulnerabilities in the DNS were found that permit an assailant to seize this procedure of gazing somebody upward or turning a webpage upward on the Internet utilizing their name. The reason for the assault is to assume responsibility for the meeting to, for instance, send the client to the criminal's own beguiling site for record and secret key assortment. These vulnerabilities have expanded enthusiasm for presenting an innovation called DNS Security Extensions (DNSSEC) to make sure about this piece of the Internet's foundation. DNSSEC will guarantee the end client is interfacing with the genuine site or other help relating to a specific space name.

[2]. INTRODUCTION

(i) Overall Description :

DNS is the shorthand for the Domain Name System. The Domain Name System provides a mechanism of conversion with a double functionality: it translates both symbolic host names to IP addresses and IP addresses to host names. The DNS has three major components: • The first category contains: – the Domain Name Space and – the Resource Records, that are specifications for a tree structured name space and the data associated with these names. • Name Servers are server programs which maintain the information about the DNS tree structure and can set information. A name server may cache information about any part of the domain tree, but in general it has complete information about a specific part of the DNS. This means the name

server has authority for that sub domain of the name space - therefore it will be called authoritative.

Resolvers are programs that extract the information from name servers in response to client requests.

The DNS was designed as a replacement for the older horse stable system both were intended to provide names for network resources atom more abstract level then network IP address in recent year the DNS has become a database of convenience for the internet with man proposes to add new features on some of these proposal have been successful in the main motivation for using DNS is because it exists and is widely deployed not because its existing structure facilities and content are appropriate for the particle application of data and what this document review the history of the DNS including examination of some of those news news anywhere application it then argue argue that the overloading process is an inappropriate, instead it suggest that the DNA should be supplemented by systems better maths 2B intended applications and outlines of frame work and rational for one such system to connect to a system that support IP the host initiating the connection was no in advance the IP address of the remote system an IP address is 32bit number that represent the location of the system on a network that 32 bit address is separated into 4 states and chocolate is typically represented by a decimal number the four decimal numbers are separated from each other by a dot character even the four decimal numbers may be easier to remember then 32 ones and zeros as with phone number there is a practical practical limit as to how many IP addresses a person can remember.

(ii) Purpose :

The DNS not only supports host name to network address resolution, known as forward resolution, but also network address to host name resolution, known as inverse resolution. This ability of mapping human memorable system names into computer network numerical addresses, its dispersed nature, and its strength, the DNS has become a vital component of the Internet. Without DNS, the only way to reach other computers on the Internet is to use the numerical network address.

(iii) Motivational and Scope :

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. 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). The message combines with the Private key to form a Signature using DSA Algorithm, which is send along with the Public key

The Domain name system has become a serious equipped part of the Internet communications, though it doesn't contain secured mechanism to guarantee data integration or verification. Extensions to DNS provides services to security awares resolves are applications through the Cryptographic digital signatures which are included as resource records and also provides

storage of valid public keys in the DNS which support general public key distribution services and also DNS security. The stored keys make security aware resolvers to know authenticating key of zone and these keys can be used to maintain other protocols and extensions gives for the authenticating DNS protocol transactions also.

DNS provides security using the concepts of Digital signature and Asymmetric key cryptography. In this asymmetric key is send as a substitute of private key. DNS security uses message digest algorithm to compact message and PRNG (pseudo random number generator) algorithm in order to generate this public and private key. Signature which is formed by combining message with the private key using DSA Algorithm is send along with public key To form a signature receiver makes use of the public key and DSA Algorithm. If the received message signature is matched then that message is decrypted and will be read or else it will be discarded.

Fig. 1: Basic DNS functionality

[5]. PROPOSED MODEL

Taking the above existing system into concern the best solution is using Pseudo Random Number Generator for generating Key Pair in a quick and more secured manner. We use MD5 (or) SHA-1 for producing Message Digest and Compressing the message. Signature is created using Private Key and Message Digest that is transmitted along with the Public Key. The transfer

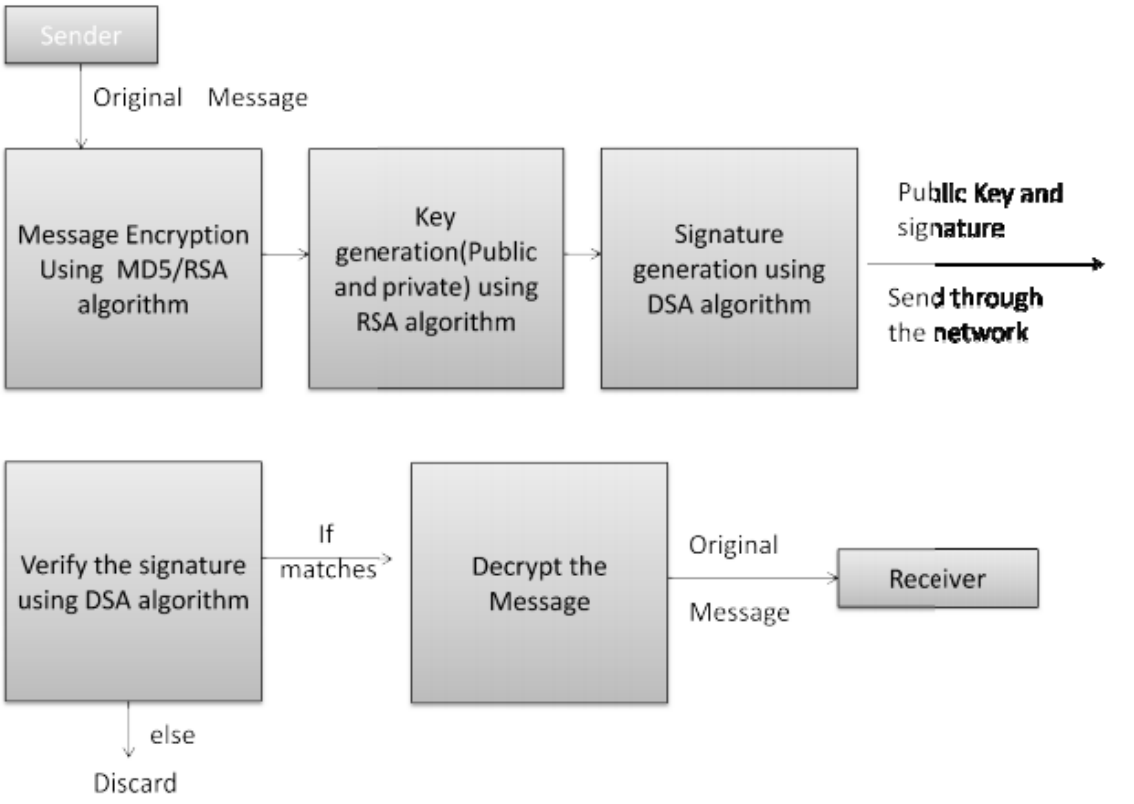
of the packets from each System to System is shown using Graphical User Interface (GUI). Each time the System get the message, it verifies the IPAddress of the sender and if match is not found then discards it. For verification, the Destination System generates Signature using Public Key and DSA Algorithm and verifies it with received one. If it matches it Decrypts else it discards.

Algorithms used :

- Message Digest
- Hashing Function
- Digital Signature

DIGITAL SIGNATURE :

A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures



HASHING FUNSTIONS :

DNS is centralized across several servers to stop the following:

1. Querying the IP for the domain name.
2. Continuously querying the domain name to do #1.
3. Changing an entry to the database.

A **Hash function** is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, digests, or

simply hashes. The values are used to index a fixed-size table called a hash table. Use of a hash function to index a hash table is called hashing or scatter storage addressing.

Hash functions and their associated hash tables are used in data storage and retrieval applications to access data in a small and nearly constant time per retrieval, and storage space only fractionally greater than the total space required for the data or records themselves. Hashing is a computationally and storage space efficient form of data access which avoids the non-linear access time of ordered and unordered lists and structured trees, and the often exponential storage requirements of direct access of state spaces of large or variable-length keys.

Hash functions are related to (and often confused with)

- Checksums,
- Check digits,
- Fingerprints,
- Lossy compression
- Randomization functions
- Error-correcting codes
- Ciphers

Although the concepts overlap to some extent, each one has its own uses and requirements and is designed and optimized differently.

- Fast and efficient work
- Ease of access to system
- Manual effort is reduced

Basic Idea of the proposed Model is based on

The Proposed model contains these main parts:

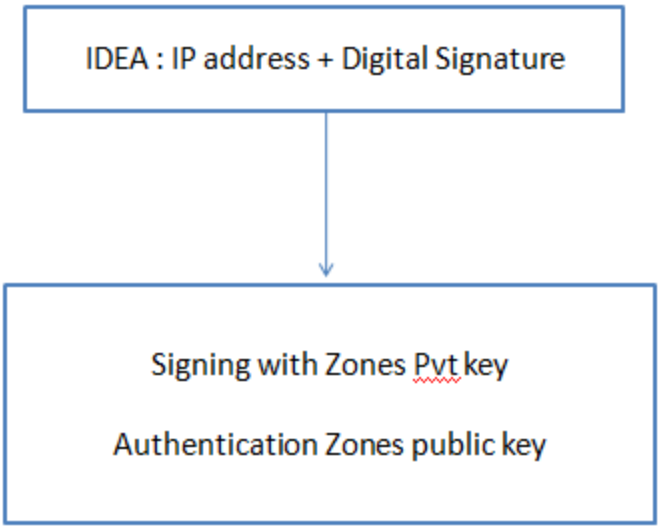
1) IP Address generation
2) Key generation
3) Signature generation
4) Signature verification

Key Generation :

Key Generation Careful generation of all keys is a sometimes overlooked but absolutely essential element in any cryptographically secure system. The strongest algorithms used with the longest keys are still of no use if an adversary can guess enough to lower the size of the likely key space so that it can be exhaustively searched. Technical suggestions for the generation of random keys.. One should carefully assess if the random number generator used during key generation adheres to these suggestions. Keys with a long effectively period are particularly sensitive as they will represent a more valuable target and be subject to attack for a longer time than short period keys. It is strongly recommended that long-term key generation occur off-line in a manner isolated from the network via an air gap or, at a minimum, high-level secure hardware.

- Encryption and Decryption,
- Signature Creation,
- Signature Verification.

Proposed Model



Zone Files Authentication :

In order to make a case for integrity checking of the zone file for improving the security of DNS, we need to take a look at the major transactions of DNS, their vulnerabilities, existing countermeasures and their limitations. The three major transactions in the DNS are:

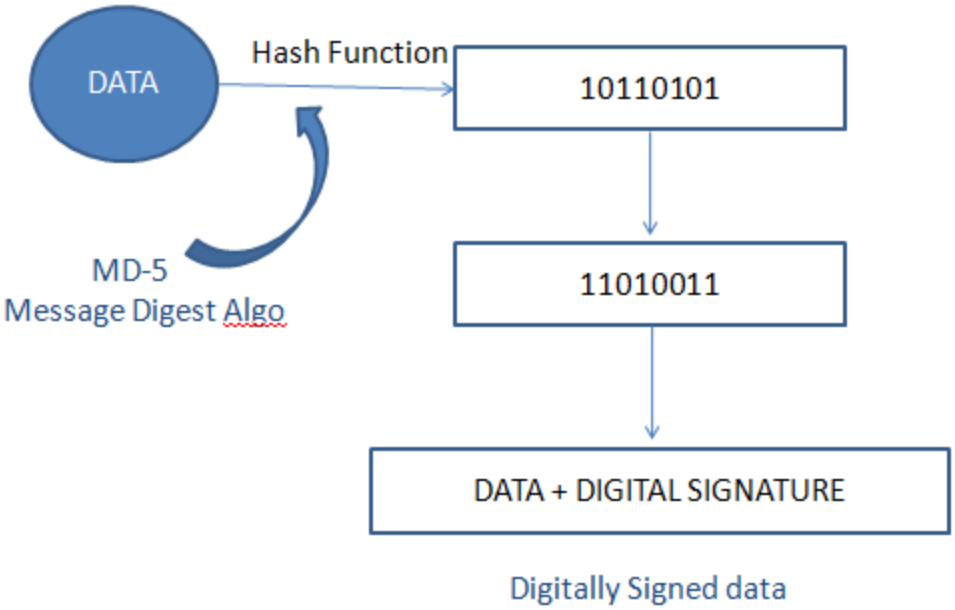
• DNS Query/Response:

This involves all name resolution queries and their associated responses

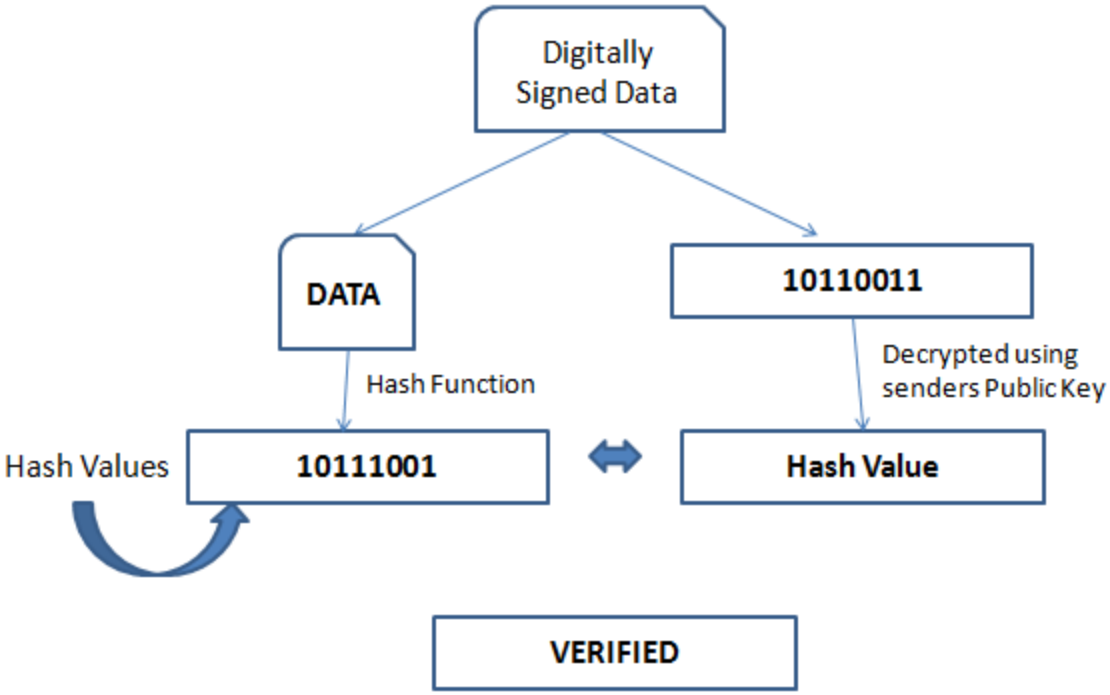
. • Zone Transfer: Transactions involving periodical refresh of the contents of zone files in secondary authoritative name servers from primary authoritative name servers.

• Dynamic Update: Update of zone file data in real time by special clients such as DHCP servers or Internet Multicast Address Servers.

Signing


DATA
Hash Function
10110101
11010011
MD-5
Message Digest Algo
DATA + DIGITAL SIGNATURE
Digitally Signed data

VERIFICATION



EXISTING SYSTEM

Authenticity is based on the identity of some entity. This entity has to prove that it is genuine. In many Network applications the identity of participating entities is simply determined by their names or addresses. High level applications use mainly names for authentication purposes, because address lists are much harder to create, understand, and maintain than name lists. Assuming an entity wants to spoof the identity of some other entity, it is enough to change the mapping between its low level address and its high level name. It means that an attacker can fake the name of someone by modifying the association of his address from his own name to the name he wants to impersonate. Once an attacker has done that, an authenticator can no longer distinguish between the true and fake entity. It is known the fact that DNS is weak in several places. Using the Domain Name System we face the problem of trusting the information that came from a non authenticated authority, the name-based authentication process, and the problem of accepting additional information that was not requested and that may be incorrect.“Many of the classic security breaches in the history of computers and computer networking have had to do not with fundamental algorithm or protocol flaws, but with implementation errors.

These are basic concepts involved in existing model ---

- The existing system is manually maintained.
- It uses RSA algorithm for key generation.
- Since it uses RSA algorithm it is necessary to provide two prime numbers to generate key pair which results in Mathematical and Brute force attack.

- It sends the public key through public network.
- Time consumption
- Low reliability

DisAdvantages

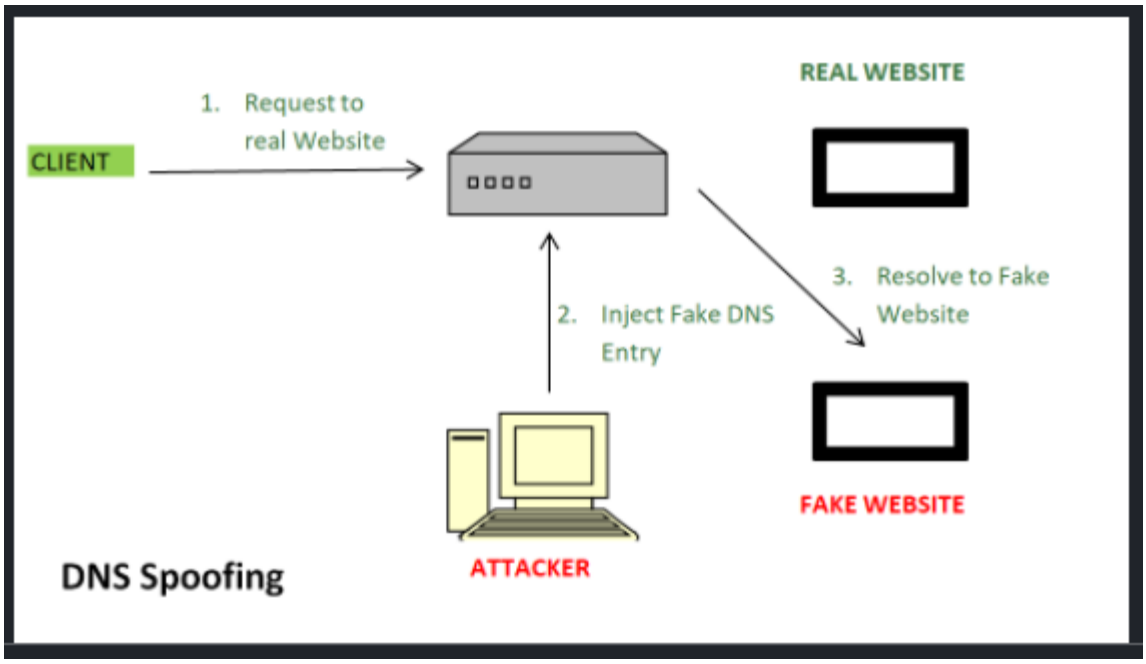
- Error prone
- Less Operational Speed
- Low speed communication

IMPLEMENTATION/ OUTPUT RESULTS

These are the basic implementation rules need to considered while getting the results.

1) Misdirected Destination: Trusting Faked Information
2) Name Based Authentication/Authorization
3) Trusting Supplementary : Non-Authoritative Information

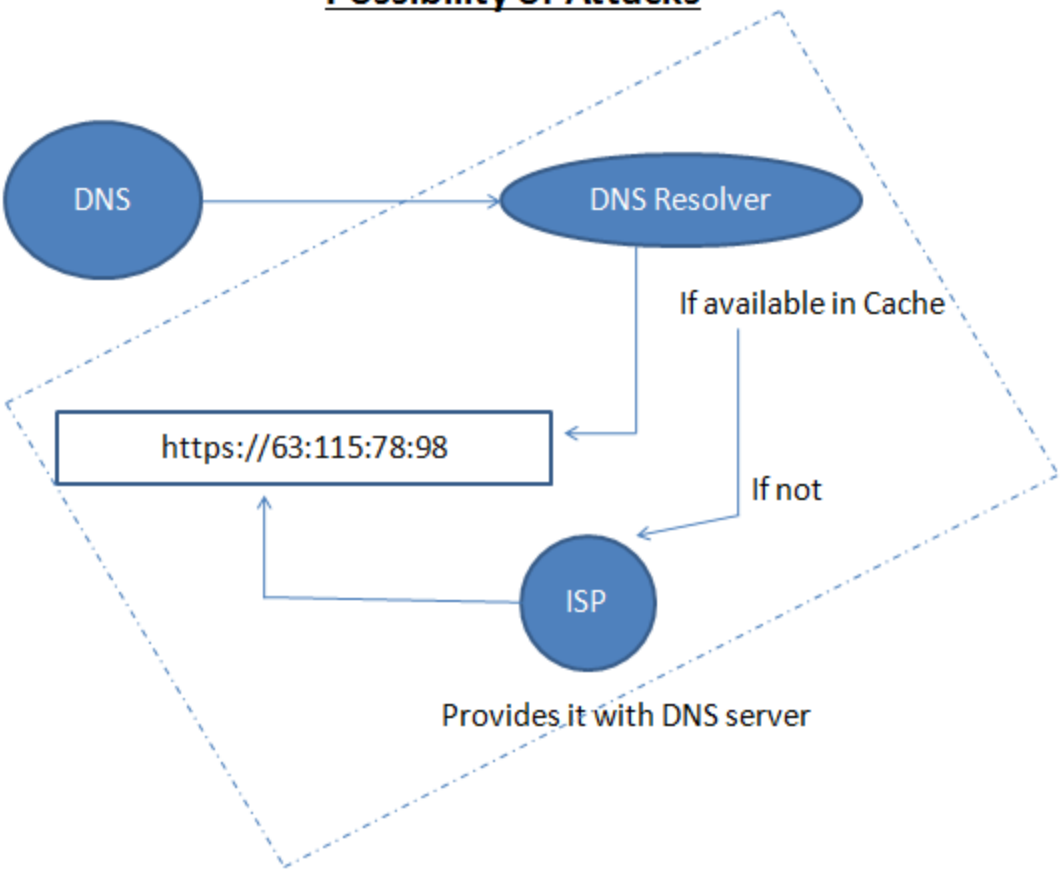
IP Spoofing :

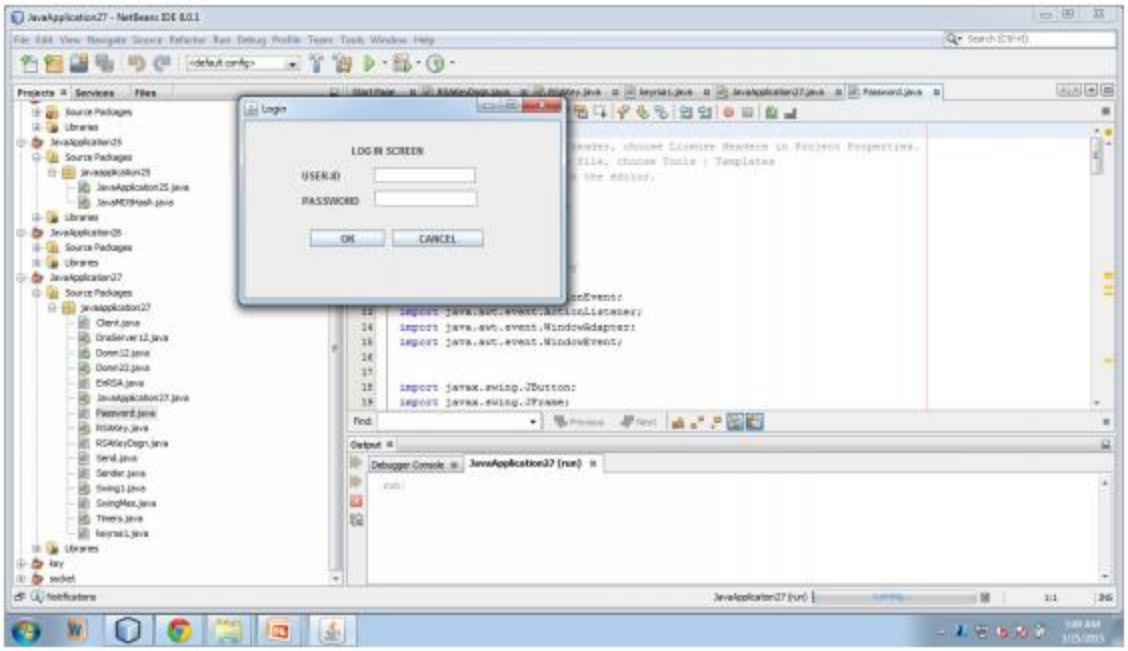


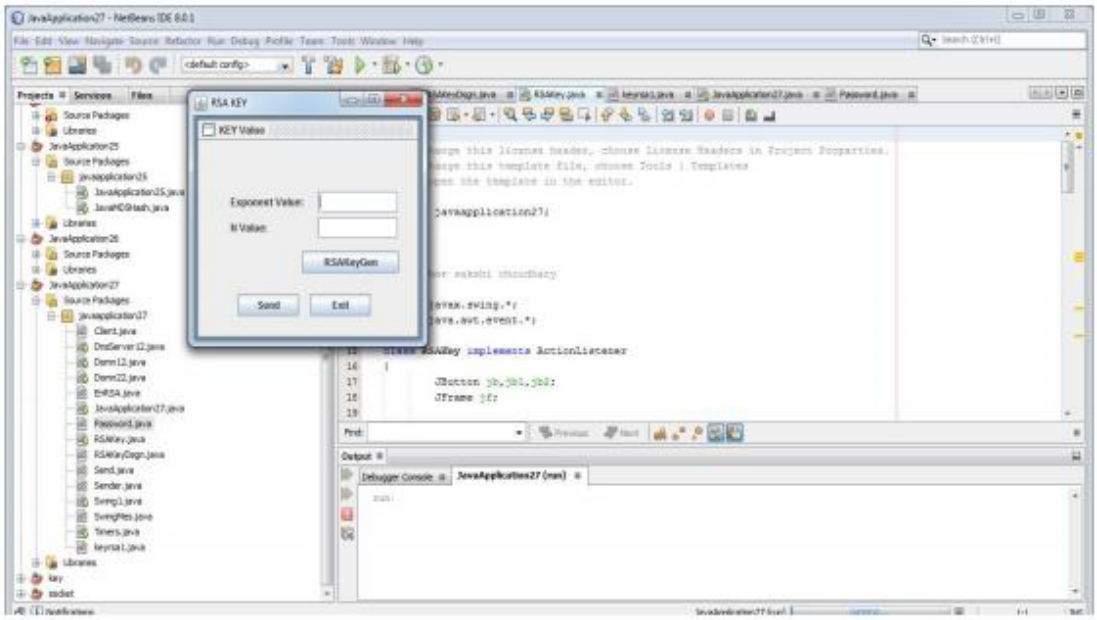
Involving Cryptography :

The need for security extensions to DNS was acknowledged and standardized in an organized manner within the DNSSEC IETF working group. The first step is to provide data authentication of the resource records travelling back and forth in the internet. With authentication come also data integrity and data source authentication. The authentication is obtained by means of cryptographic digital signatures. The public key algorithms used for authentication in DNSSEC are MD5/RSA and DSA. The digital signatures generated with public key algorithms have the advantage that anyone having the public key can verify them. Each resource record in the DNS messages exchanged can be digitally signed providing data origin authentication and integrity of the message.

Possibility of Attacks




JavaApplication27 - NetBeans IDE 8.0.1
Login
LOG IN SCREEN
USER ID
PASSWORD
OK
CANCEL


JavaApplication27 - NetBeans IDE 8.0.1
RSA KEY
KEY Value
Exponent Value:
N Value:
RSAKeyGen
Send
Exit

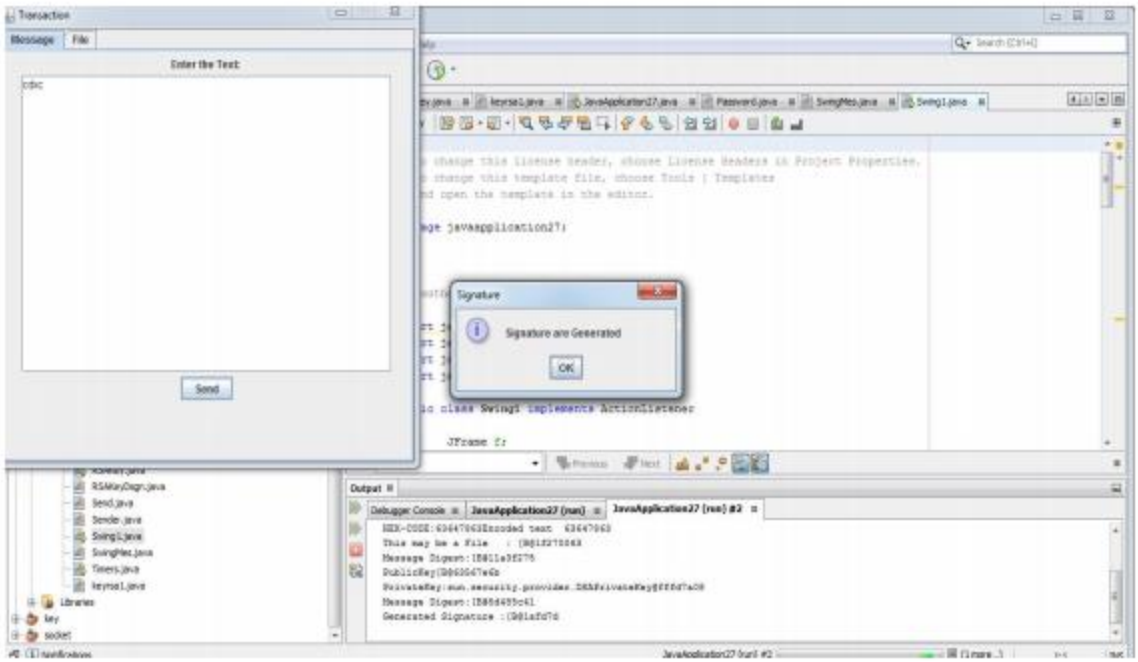


Figure 9:Signature generation

CONCLUSION

The DNS as an Internet standard to comprehend the issues of versatility encompassing the hosts.txt record. From that point forward, the across the board utilization of the DNS and its capacity to determine have names into IP addresses for the two clients and applications the same in an opportune and genuinely solid way, makes it a basic segment of the Internet. The dispersed administration of the DNS and backing for repetition of DNS zones over different servers advances its vigorous attributes. Be that as it may, the first DNS convention particulars did exclude security. Without security, the DNS is defenseless against assaults originating from store harming strategies, customer flooding, dynamic update vulnerabilities, data spillage, and bargain

of a DNS server's definitive documents. So as to add security to the DNS to address these dangers, the IETF added security expansions to the DNS, by and large known as DNSSEC. DNSSEC gives validation and uprightness to the DNS. Except for data spillage, these expansions address most of issues that make such assaults conceivable. Store harming and customer flooding assaults are relieved with the expansion of information root validation for RR Sets as marks are registered on the RR Sets to give verification of credibility. Dynamic update vulnerabilities are alleviated with the expansion of exchange and solicitation validation, giving the fundamental confirmation to DNS servers that the update is true. Indeed, even the risk from bargain of the DNS server's legitimate records is nearly wiped out as the SIG RR are made utilizing a zone's private key that is kept disconnected as to guarantee key's trustworthiness which thus shields the zone document from 28 altering. Keeping a duplicate of the zone's lord document disconnected when the SIGs are produced makes that affirmation one stride further. DNSSEC can not give insurance against dangers from data spillage. This is a greater amount of an issue of controlling access, which is past the extent of inclusion for DNSSEC. Sufficient insurance against data spillage is as of now gave through such things as split DNS design. DNSSEC shows some encouraging ability to shield the Internet foundation from DNS based assaults. DNSSEC has some genuinely entangled issues encompassing its turn of events, setup, and the board.

[6]. References

[1] Hu Junru, “The Improved Elliptic Curve Digital Signature Algorithm”, International Conference on Electronic & Mechanical Engineering and Information Technology, IEEE, 2011

[2] Casey Deccio, Jeff Sedayao and Krishna Kant, Prasant Mohapatra, ”Quantifying and Improving DNSSEC Availability’, IEEE, 2011.

[3] Ghanmy Nabil, Khlif Naziha, “Hardware implementation of Elliptic Curve Digital Signature Algorithm (ECDSA) on Koblitz Curves” 8th IEEE, IET International Symposium on Communication Systems, Networks and Digital Signal Processing, IEEE, 2012.

[4] 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, 10th April 2013.

[5] Aqeel Khalique, Kuldip Singh, Sandeep Sood, “Implementation of Elliptic Curve Digital Signature International Journal of Computer Applications (0975 – 8887) Volume 120 – No.17, June 2015 15 Algorithm”, International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010 [6] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, Elliptic Curve Cryptography, May 20-26, 2008. ACM Ubiquity, Volume 9, Issue 20.

[7] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang, “High-speed high-security signatures”, 2011.

[8] HONG Jingxin, “A New Forward-Secure Digital Signature Scheme”, IEEE, 2007.

[9] El hadj youssef wajih, Machhout Mohsen, “A Secure Elliptic Curve Digital Signature Scheme for Embedded Devices”, International Conference on Signals, Circuits and Systems, IEEE, 2008.

[10] Xue Sun, Mingping Xia, “An Improved Proxy Signature Scheme Based on Elliptic Curve Cryptography”, International Conference on Computer and Communications Security, IEEE, 2009.

[11] Jonathan Petit, “Analysis of ECDSA Authentication Processing in VANETs”, IEEE, 2009.

[12] Qingkuan Dong, Guozhen Xiao, “A Subliminal-Free Variant of ECDSA Using Interactive Protocol”, IEEE, 2010.

[13] Jalel Ben-othman, Yesica Imelda Saavedra Benitez, “A light weight security scheme for HWMP protocol using Elliptic Curve Technique”, 11th IEEE International Workshop on Wireless Local Networks, IEEE, 2011.

[14] M. Janagan, M. Devanathan, “Area Compactness Architecture for Elliptic Curve Cryptography”, International Conference on Pattern Recognition, Informatics and Medical Engineering, March 21-23, IEEE, 2012.

[15] Zhang Youqiao ,Zhou Wuneng, “An ECDSA Signature Scheme Designs for PBOC 2.0 Specifications”, 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012), IEEE, 2012.

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

[17] Nabil GHANMY, Lamia CHAARI FOURA TI, Lotfi KAMOUN, “Enhancement security level and hardware implementation of ECDSA”, IEEE, 2013.

[18] Soumya Basu, M.Pushpalatha, “Analysis of Energy Efficient ECC and TinySec Based Security Schemes in Wireless Sensor Networks”, IEEE, 2013.

[19] Shweta Lamba, Monika Sharma, “An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA)”, International Conference on Machine Intelligence Research and Advancement, IEEE, 2013. [20] Noura Ben Hadjy Youssef, Wajih El Hadi Youssef , Mohsen Machhout, Rached Tourki, “A Low-Resource 32-bit Datapath ECDSA