SECURITY SYSTEM FOR DNS USING CRYPTOGRAPHY

Progress Report

In fulfillment of the requirements for the

NU 302 R&D Project

At NIIT University



Submitted by

Padegal Sai Giriraj

Naman Shah

Vivek singh

Navneeth rao

Ashish singh

Area

NIIT University

Neemrana

Rajasthan

**CERTIFICATE**

This is to certify that the present research work entitled " **Security system for dns using cryptograph**y” being submitted to NIIT University, Neemrana, Rajasthan, in the fulfillment of the requirements for the course at NIIT University, Neemrana, embodies authentic and faithful record of original research carried out by **P Sai giriraj,Naman shah,Vivek singh,Navneeth rao,Ashish singh**, student/s of B Tech (**CSE**) at NIIT University, Neemrana,. She /He has worked under our supervision and that the matter embodied in this project work has not been submitted, in part or full, as a project report for any course of NIIT University, Neemrana or any other university.

Name and Title of the Mentor :

Mr Abdul Mazid

**CONTENTS**

Title Page no.

Certificate

List of Figures

List of Tables

Rational

Literature Review

Objectives

Methodology

Results

Summary

Future Work

References

**SECURITY SYSTEM FROM DNS USING CRYPTOGRAPHY**

Naveen Kumar Tiwari

Sanjay Khakhil

**Abstract :**

DNS, Domain Name System is a convention that purposes hostnames to IP Addresses over the Internet. DNS, being an open source, it is less secure and it has no methods for deciding if domain name information originates from an approved domain proprietor. In this way, these vulnerabilities prompt various assaults, for example, reserve harming, store caricaturing and so forth. Subsequently, there is a need of securing DNS. Advanced Signatures are a decent method for authenticating the domain proprietors. The paper exhibits the Domain Name System security idea,. Computerized Signature calculations helps in giving great level of security to DNS. Programming like OpenDNSSEC, BIND, Secure64 and so on. It includes the marking of DNS utilizing cryptographical calculations (e.g., RSA, DSA and so on.). Further, ECDSA is one way that gives same level of security, as security gave by RSA to low power and versatile gadgets. In this way, here we proposing another ECDSA execution that can be utilized to secure DNS. The motivation behind this work is to demonstrate the recreation of how these product system functions, yet with ECDSA calculation actualized in it. ECDSA being quick at checking the marks and uses little key size when contrasted with RSA and furthermore, gives same level of security as given by RSA. ECC is a developing field of future.. Along these lines, this work includes DNS security utilizing ECC. ECC being exceptionally secure, littler key sizes, less in power and memory utilization gives better security to compact little gadgets.

**Algorithms used :**

1)Elliptic curve cryptography [ECC]

2)Digital Signature algorithm [DSA]

**Methodology :**

Steps Followed :

1)Selecting key parameters required for ECDSA algorithm

2)Signature generation

3)Signature verification

**Algorithm comparison :**

|  |  |  |
| --- | --- | --- |
| **PARAMETERS** | **RSA** | **ECDSA** |
| Key Size | 1024 bit length | 192 bit length smaller |
| Encryption | Fast | Slow |
| Decryption | Slow | Fast |
| Key Exchange | Fast | Slow |
| Signature generation | Slow | Fast |
| Signature Verification | Fast | Slow |

**Conclusion :**

The reason for this work is to demonstrate the simulation of how

these product system works, however with ECDSA calculation executed in it. ECDSA being quick at checking the marks and uses little key size when contrasted with RSA and likewise, gives same level of security as given by RSA. ECC is a developing field of future.. Along these lines, this work includes DNS security utilizing ECC. ECC being exceptionally secure, littler key sizes, less in power and memory.

**Security System for DNS using Cryptography**

Sachin Kumar Sinha

Avinash Kant Singh,

Amaresh Sharma

**Abstract :**

The mapping or authoritative of IP delivers to have names turned into a noteworthy issue in the quickly developing Internet and the more elevated amount restricting exertion experienced distinctive phases of advancement up to the right now utilized Domain Name System (DNS).The DNS Security is intended to give security by joining the idea of both the Digital Signature and Asymmetric key (Public key) Cryptography. Here the Public key is send rather than Private key. The DNS security utilizes Message Digest Algorithm to pack the Message(text record) and PRNG(Pseudo Random Number Generator) Algorithm for creating Public and Private key. The message consolidates with the Private key to frame a Signature utilizing DSA Algorithm, which is send alongside the Public key.The beneficiary uses the Public key and DSA Algorithm to shape a Signature. In the event that this Signature matches with the Signature of the message got, the message is Decrypted and perused else disposed of.

**Algorithms :**

1)Message DIgest Algorithm[to compress message]

2)Pseudo Random Number Generator[Private & Public key Generator]

**Methodology :**

According to research paper best arrangement is utilizing Pseudo Random Number Generator for creating Key Pair in a snappy and more secured way. They utilize MD5 (or) SHA-1 for delivering MessageDigest and Compressing the message.Signature is made utilizing Private Key and MessageDigest which is transmitted alongside the Public Key. The exchange of the bundles from each Framework to System is demonstrated utilizing Graphical User Interface (GUI). Each time the System get the message, it checks the IP Address of the sender and if no match is discovered it disposes of it. For confirmation, the Destination System creates Signature utilizing PublicKey and DSA Algorithm and checks it with got one. In the event that it matches it Decrypts else it disposes of.

**Conclusion :**

Keeping in mind the end goal to add security to the DNS to address these dangers, the IETF added security expansions to the DNS, on the whole known as DNSSEC. DNSSEC gives verification and trustworthiness to the DNS. Except for data spillage, these augmentations address the lion's share of issues that make such assaults conceivable. Reserve harming and customer flooding assaults are relieved with the expansion of information cause confirmation for RRSets as marks are registered on the RRSets to give evidence of legitimacy. Dynamic refresh vulnerabilities are alleviated with the expansion of exchange and demand confirmation, giving the vital affirmation to DNS servers that the refresh is genuine. Indeed, even the danger from trade off 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 uprightness which thus shields the zone document from altering. Keeping a duplicate of the zone‟s ace document disconnected when the SIGs are produced makes that confirmation one stride further.

**A Framework for Security of DNS using Cryptography**

Naveen Kumar

Kamal Kumar Ranga

**Abstract :**

DNS, Domain Name System is a convention that purposes hostnames to IP Addresses over the Internet. DNS, being an open source, it is less secure and it has no methods for deciding if domain name information originates from an approved domain proprietor. Along these lines, these vulnerabilities prompt various assaults, for example, store harming, reserve ridiculing and so on. Consequently, there is a need of securing DNS. Computerized Signatures are a decent method for verifying the domain proprietors. The computerized marks created with open key calculations have the favorable position that anybody having general society key can check them. Existing proposition incorporate open key cryptographic calculations (e.g., RSA, DSA and so on.) for securing DNS. With the innovation becoming quicker everybody gets to web through cell phones whether it is utilized to check E-Mails or going to any safe locales, ECDSA including ECC (Elliptic Bend Cryptography) ideas having less key sizes when contrasted with RSA can be actualized to give security to DNS.

**Methodology :**

Steps Followed :

1)Key Pair Generation

2)Signature Generation

3)Signature Verification

**Conclusion :**

There are different safety efforts received in DNS utilizing public key cryptography, which incorporates RSA and DSA. With the innovation developing step by step, there is a need of same level of security with littler key sizes. Presently, everybody utilizes versatile to recover information from web and versatile being little and compact gadget needs security with less power utilization. This can be finished with the assistance of ECC by executing ECDSA in DNS. Likewise, these days everybody utilizes their advanced mobile phones to remove substance from the Internet. Regardless of whether telephones are utilized for opening different sites, accepting messages, topping off online structures and so on., working these colossal RSA secured web content is time and memory devouring both. In this way, there is a need of quicker verifier on these little handheld gadgets to verify the web sources rapidly and with less power and memory utilization. The capacity of speedy confirmation with little piece sizes of keys utilized is given by ECDSA.

**Security System for DNS Using Cryptography**

Lalith Amudala

Sai Gopal Polsani

Ashwath Anand L

Vignesh

Lavanya

**Abstract :**

The Domain Name System (DNS) changes over the Internet area and host names to IP locations and the other way around.

DNS changes over the names we compose in our Web program deliver bar to the IP locations of Web servers of destinations. Numerous organizations utilize DNS to deal with their own system.. In this paper they utilized cryptography (DES encryption) to execute the proposed demonstrate. In DES, a similar key is utilized to scramble and decode a message, so both the sender and the recipient should know and utilize a similar private key. The DES is a square figure, which implies that a cryptographic key and calculation are connected to a piece of information one piece at any given moment as opposed to all the while. For a plaintext message to be encoded, DES bunches it into 64-bit squares. Each piece is en-figured utilizing the mystery enter into a 64-bit figure content utilizing stage and substitution. This procedure includes 16 adjusts and can keep running in four different modes, by encoding pieces separately or making each figure piece reliant on all their past squares. Unscrambling is basically the turn around of encryption, where similar advances are taken after however turning around the request in which the keys are connected. The most fundamental technique for assault for any figure is beast constrain, which includes attempting each key until the point that you locate the correct one.

**Algorithms Used :**

1)DES Encryption

2)CORBA [Common Object Request Broker Architecture]

**Conclusion :**

This clarifies the worries in different differences that are looked in the present relationship of information excess and speed enhancement. Security and speed are settled from our clarification through issue proclamation with additional middleware incorporated into the procedure which helps weight on framework which expands speed of which look

calculations work at its high potential and from which cost is decreased on DNS frameworks at the end of the day expanded on middleware components.We still mean to make improvements in the future by enhancing the speed and proficiency of the procedure in order to give a quicker client experience and furthermore to battle developing dangers.

**Security of the DNS Protocol Implementation and Weaknesses Analyses of DNSSEC**

Kaouthar Chetioui,

Ghizlane Orhanou,

Said El Hajji,

Abdelmajid Lakbabi

**Abstract :**

Today, Internet offers many critical applications. So, it becomes very crucial for Internet service providers to ensure traceability of operations and to secure data exchange. Since all these communications are based on the use of the Domain Name System (DNS) protocol, it becomes necessary to think to enhance and secure it by proposing a secure version of this protocol that can correct the whole or a part of the DNS protocol weaknesses and vulnerabilities. In this context, DNSsec was created by the IETF to ensure the integrity of DNS data and authentication of the source of such data. DNSsec is based on the key cryptography public to provide different security services. In the present paper, we will present first the DNS protocol and its weaknesses. After that, we will be interested in studying the DNSsec implementation and data exchange, and then give a deep analysis of its weaknesses.

**WEAKNESSES AND PROSPECTS OF DNSSEC :**

The DNSSECconvention have tackled numerous security issues of the DNS convention by giving validation and information uprightness yet it is

still defenseless against a few sorts of assaults. By including asset

records to secure exchanges, the extent of a DNSSEC zone document end up seven times bigger than that of a DNS record. Moreover, the DNSSEC convention will utilize TCP convention and not UDP. This will cause an expansion of the system stack.Also, up to now, there is no vigorous framework that can confront a Denial of Service assault. Hence, given the size DNSSEC messages there is as yet defenseless. DNSSEC does not ensure unsigned records, so we need to consider securing the zone exchange by different strategies. What's more, DNSSEC should be synchronized between the customer and the element making the synchronization, so amid this stage, there could be an interference of records and the same issue can be arised amid the keys reestablishment.

**Conclusion :**

Today, Internet offers many critical applications. So, it becomes very crucial for Internet service providers to ensure traceability of operations and to secure data exchange. Since all these communications are based on the use of the Domain Name System (DNS) protocol, it becomes necessary to think to enhance and secure it by proposing a secure version of this protocol that can correct the whole or a part of the DNS protocol weaknesses and vulnerabilities. In this context, DNSsec was created by the IETF to ensure the integrity of DNS data and authentication of the source of such data. DNSsec is based on the key cryptography public to provide different security services. In the present paper, we will present first the DNS protocol and its weaknesses. After that, we will be interested in studying the DNSsec implementation and data exchange, and then give a deep analysis of its weaknesses.