Government Engineering College

Bikaner

Computer Science & Engineering Department

A

Project Synopsis

On

**“Security System For DNS Using Cryptography”**

**Guided By:**

Deepika Ma’am

**Team Submitted By:**

Hawa Singh, B.tech (CSE), IV Year,

kasanahawa@gmail.com

Madhur Dhodria, B.tech(CSE),IV Year

Madhurdhodria96@gmail.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 currently used Domain 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.

**INTRODUCTION**

**SCOPE OF THE PROJECT**:

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) 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.

**PROBLEM STATEMENT:**

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. 0nce an attacker has done that, an authenticator can no longer distinguish between the true and fake entity.

**PROPOSED SYSTEM :**

Taking the above prevailing system into consideration 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 which 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 IP Address of the sender and if no match is found it 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 otherwise it discards.

The Following function avoids the pitfalls of the existing system.

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

**DEVELOPMENT ENVIRONMENT:**

**HARDWARE ENVIRONMENT:**

The minimum configuration required to run this project are:

1. Main processor :Pentium III (or) IV and Above version
2. RAM : Minimum 128 M
3. Hard Disk : Minimum 4.2 GB
4. Clock Speed : 550 MHZ
5. System Bus Speed : 400 MHz
6. Cache RAM : 256 KB

**SOFTWARE ENVIRONMENT:**

Language : JDK 1.3 or Higher.

Front End Design : Swings

Operating System : Windows

Technologies : J2SE (network, IO, Swing, Util, Cryp.)