DNSSEC
An Overview

H S Gupta
Earlier DGM in BSNL
hari.gupta@in.ibm.com

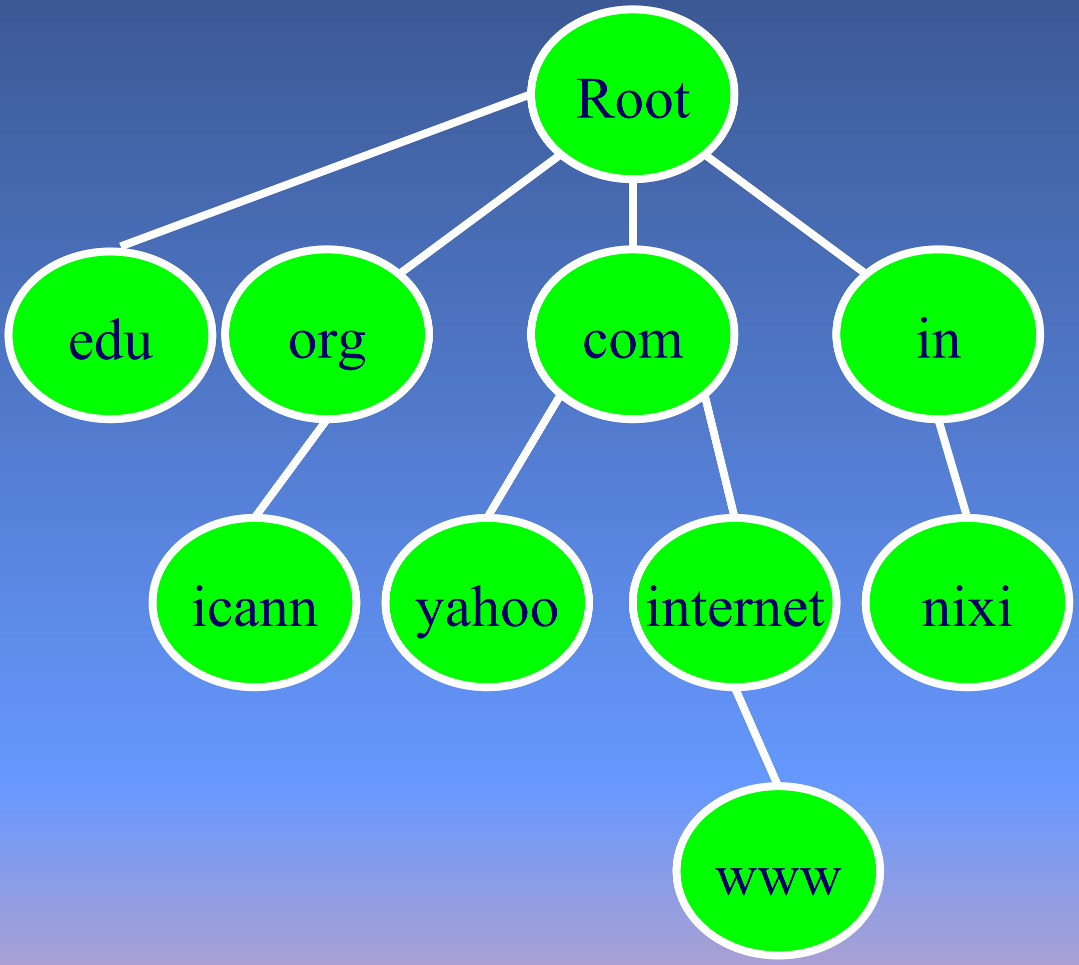
Domain Name System

- Basically provides mappings for Name to IP and vice versa (www.icann.org=208.77.188.103)
- Critical for Internet Operations
- Globally distributed Database

Domain Name System

Data is organized in

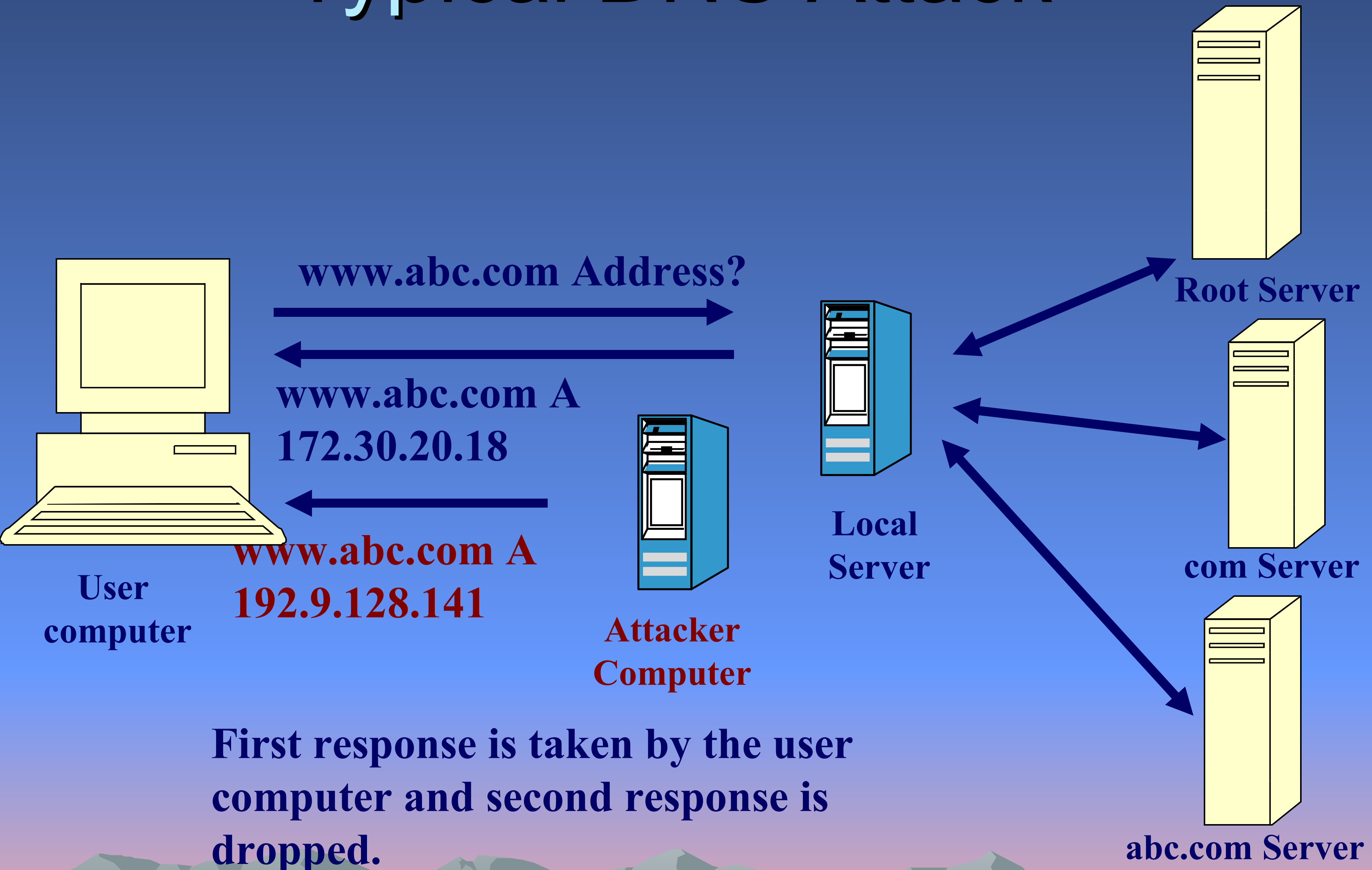
tree like structure



Problem

- DNS is vulnerable to spoofing attack
- No authentication is available
- Resolver does not distinguish between valid and invalid data

Typical DNS Attack



www.abc.com Address?

www.abc.com A 172.30.20.18

www.abc.com A 192.9.128.141

User computer

Attacker Computer

Local Server

Root Server

com Server

abc.com Server

First response is taken by the user computer and second response is dropped.

DNSSEC

- Digital Signature framework. Application of Public Key Cryptography
- Adds Data origin authentication that is Data the DNS user receives came from correct originator
- Adds Data integrity that is Data received is the Data the originator put into the DNS
- Makes spoofing detectable by end user (resolver)

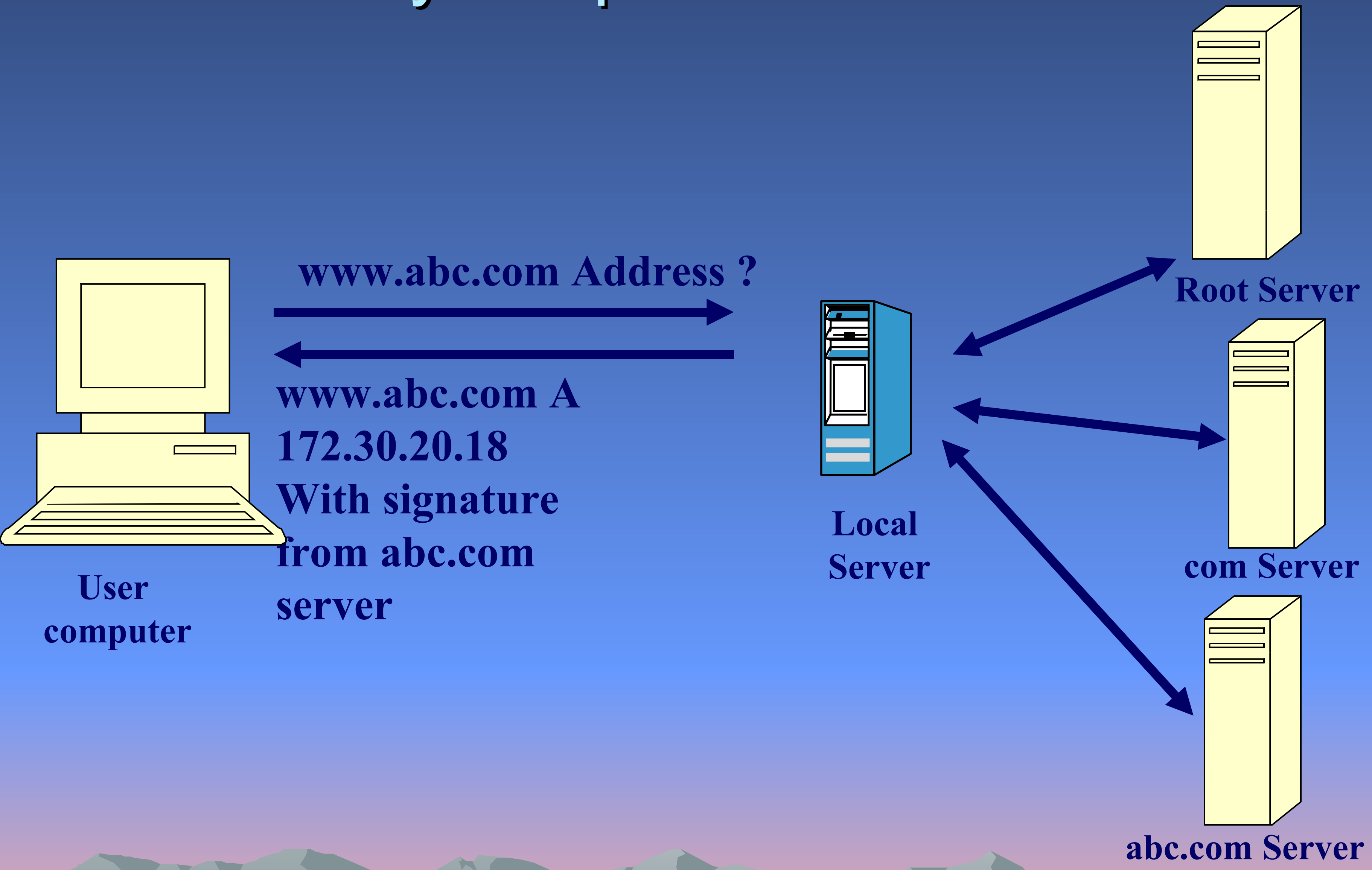
DNSSEC

- Each DNS zone signs their data with private key
- Query for a particular record returns the requested RRSet and the SIG of the requested RRSet
- Users authenticate responses with trusted keys (At least one trusted public key is pre configured)

DNSSEC

- Key hierarchy is built within DNS itself
- DNSSEC is about Digital Signatures not encryption
- Does not address DDoS Attacks

DNS Query Response with DNSSEC



www.abc.com Address ?

www.abc.com A 172.30.20.18 With signature from abc.com server

User computer

Local Server

Root Server

com Server

abc.com Server

Hurdles

- Complex in nature
- Additional burden on resolvers and Name servers
- Additional tasks of key management, record signing and managing zone updates
- Lack of knowledge about DNSSEC
- Very little adoption
- Signing of the root zone
- Development and deployment of DNSSEC has taken considerable time

Interim

- Increase the awareness and knowledge of DNSSEC
- Pilot testing of DNSSEC with users needs to be done
- Study of business & technical issues
- Use of alternative approaches like DNSSEC Lookaside Validation till solution for signing of root zone
- Need to move forward to make Internet Secure

Thank You