DNSSEC

by

Steven Dormady

An Independent Study Project

Department of Computer Science

James Madison University

Department of Computer Science

April 2026

Contents

Abstract

Your abstract here...

Introduction

1.1 Motivation

DNS by itself is insecure and vulnerable to attack. With DNSSEC, these vulnerabilities are contained and mitigated.

Test below Why DNSSEC matters...[1]

1.2 Problem Statement

1.3 Contributions

What you contribute...

Background

2.1 DNS Research

Firstly, I think a bit of background about DNS helps to understand why it became what it is today. DNS started as ARPANET, which mapped names to addresses using a host file that was distributed to all entities whenever changes occurred. As it may seem, this system became rapidly unsustainable once there were over 100 networked entities, which led to DNS today.[2]

In my research about DNS, I learned a lot about what happens behind the scenes with DNS Servers. Cloudflare called it, ”DNS is like the phone book of the internet.” [1] All network systems operate with network addresses, such as IPv4 and IPv6. More or less, DNS translates domain names, like www.example.com, to IP addresses, like 127.0.0.1, so browsers can load internet resources.

DNS naming system is organized as a tree structure made up of multiple levels and naturally creates a distributed system. Each node in the tree is given a label which defines its Domain (its area or zone) of Authority. The topmost node in the tree is the Root Domain; it delegates to Domains at the next level which are generically known as the Top-Level Domains (TLDs). They in turn delegate to Second-Level Domains (SLDs), and so on. The Top-Level Domains (TLDs) include a special group of TLDs called the Country Code Top-Level Domains (ccTLDs), in which every country is assigned a unique two-character country code. Below is a diagram demonstrating this hierarchyfigure 2.1.[2]

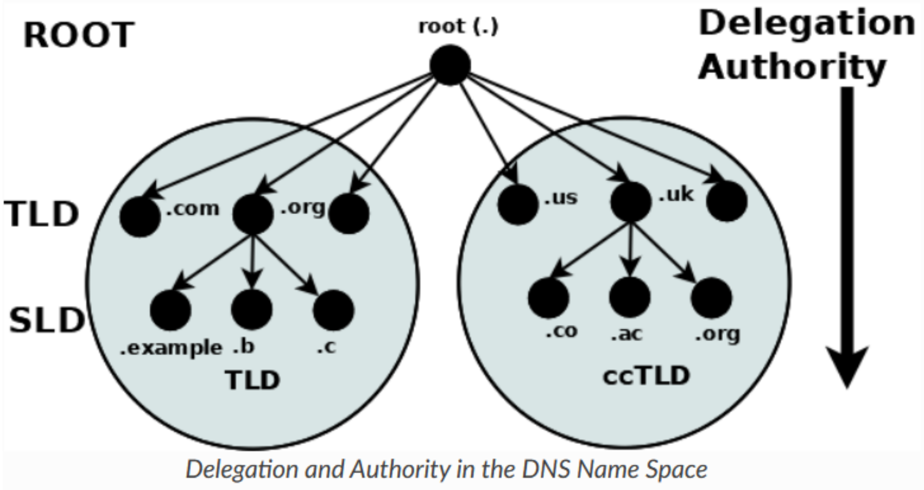
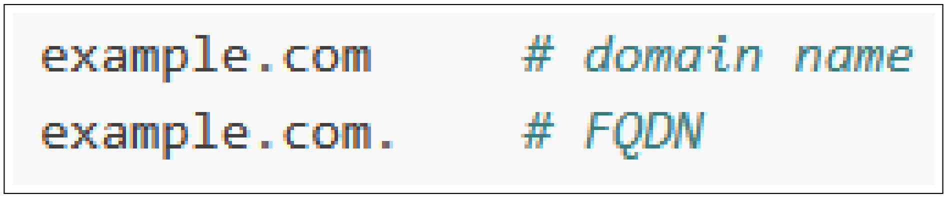


Figure 2.1: Test

A domain is the label of a node in the tree. A domain name uniquely identifies any node in the DNS tree and is written, left to right, by combining all the domain labels (each of which are unique within their parent's zone or domain of authority), with a dot separating each component, up to the root domain. In the above diagram the following are all domain names: example.com, b.com, ac.uk, us, and org. The root has a unique label of "." (dot), which is normally omitted when it is written as a domain name, but when it is written as a Fully Qualified Domain Name (FQDN) the dot must be present. As seen in figure 2.2:[2]



```
example.com      # domain name
example.com.     # FQDN
```

Figure 2.2: FDQN example, the dot on the far right making it FQDN

With this,

These root servers play a critical part of the DNS authoritative infrastructure. There are 13 root servers, which is historically tied with IPv4 data that could be packed into a 512-byte UDP message. This data limit is no longer an issue with all root servers supporting IPv4 and IPv6. In addition, almost all the root servers use anycast, with well over 300 instances of the root servers now providing service worldwide. The root servers are the starting point for all name resolution within the DNS.[2]

2.1.1 DNS Server Setup

2.1.2 DNS Vulnerabilities

2.2 VM Research

I have never dealt directly with Virtual Machines before, and building a network of them was something I had never really thought about. However, the thought excited me and it seemed like a great opportunity to learn a new skill.

The software I used to set up the testbed network for my DNSSEC program was VMWare,

Bibliography

[1] Cloudflare Learning, “What is dns?.” https://www.cloudflare.com/learning/dns/what-is-dns/, 2025. Accessed: 2025-12-22.

[2] BIND9, “Introduction to dns and bind 9.” https://bind9.readthedocs.io/en/v9.20.17/chapter1.html#the-domain-name-system-dns, 2023. Accessed: 2026-1-1.