FULLY INTEGRATED SOFTWARE DEFINED NETWORKING FOR SECURE DNS

RAMILA AKMAL

BEng

2020

Abstract

Recently technology DNS plays a major role in assisting the Internet infrastructure by offering a centralized and reliable system for resolving Internet domain names in IP addresses and IP addresses back in domain names. However, because the DNS program is generated as a public database, security vulnerabilities can be exploited. Client flooding, cache poisoning, information exposure, information leakage, DNS amplification attacks, and DNS dynamic update vulnerabilities are some of the key threats to the DNS. Taking advantage of these vulnerabilities will result in financial losses, denial of services and data manipulation and disclosure of confidential information.

With the development of the web industry security is highly needed. In this project mainly focus to implement a system for securing DNS to be protected against the vulnerabilities. The proposed system contains a solution that concerns client flooding, cache poisoning, DNS amplification attacks, and information leakage. The proposed protected DNS server needs to test the reliability and validity of the public DNS responses it receives. The server can only retain the correct DNS information in the cache. This will ensure customers receive only the most authentic DNS responses.

In the proposed system the secure DNS server must be introduced only after sufficient authentication to provide services to the clients. To prevent the attacker from spoofing an IP address of a victim host, the server must create a secure connection with the client device.