Framework for Domain Name System Security Extensions (DNSSEC) to Support the IPv6 Infrastructure

Abstract:

The major problem in DNS as originally specified in RFC 1035 is that it does not offer any form of security and it is vulnerable to spoofing, man-in-the-middle and cache poisoning attacks. This kind of attacks can compromise all communications to the host that initiate any connection that requires address translation. The threats from a certain attack on DNS are common and although several tools or devices have been introduced, it still needs to have a better solution in overcoming the issues. At the same time, there are several factors that preventing a widespread implementation of the DNSSEC, such as security testing, performance evaluation and used functionality testing. This paper proposed a framework and an implementation of DNSSEC on IPv6 environment based on the specifications for iDNSSEC on RFC 4033, 4044 and 4055. This implementation of the DNSSEC framework on IPv6 environment provides origin authentication of DNS data, data integrity, and authenticated denial of existence to protect the internet infrastructure further from malicious attacks. The prototype functionality and security testing and the performance evaluation are also presented in this paper.