Secure Domain Name System (DNS) Deployment Guide

Download EBOOK
This document provides deployment guidelines for securing the Domain Name System (DNS) in any enterprise, a government agency, or a corporate entity. The deployment guidelines follow from an analysis of security objectives and consequent protection approaches for all DNS components. This document was originally published in May 2006. Since then, the following IETF RFCs, FIPS, and NIST Cryptographic guidance documents have been published, and this revision takes into account the specifications and recommendations found in those documents - DNNSEC Operational Practices (RFC 4641), Automated Updates for DNS Security (DNSSEC) Trust Anchors (RFC 5011), DNS Security (DNSSEC) Hashed Authenticated Denial of Existence (RFC 5155), HMAC SHA TSIG Algorithm Identifiers (RFC 4635), The Keyed-Hash Message Authentication Code (HMAC) (FIPS 198-1), Digital Signature Standard (FIPS 186-3), and Recommendations for Key Management (SP 800-57P1 & SP 800-57P3). In addition, this revision provides illustrations of Secure configuration examples using DNS Software, offering NSD, in addition to BIND, guidelines on Procedures for migrating to a new Cryptographic Algorithm for signing of the Zone (Section 11.5), guidelines for Procedures for migrating to NSEC3 specifications from NSEC for providing authenticated denial of existence (Section 11.6) and deployment guidelines for Split-Zone under different scenarios (Section 11.7).

Dmca