Network Working Group   D. Eastlake
Request for Comments: 2535   IBM
Obsoletes: 2065   March 1999
Updates: 2181, 1035, 1034
Category: Standards Track

                 Domain Name System Security Extensions

Status of this Memo

Copyright Notice

Abstract

   Extensions to the Domain Name System (DNS) are described that provide
   data integrity and authentication to security aware resolvers and
   applications through the use of cryptographic digital signatures.
   These digital signatures are included in secured zones as resource
   records. Security can also be provided through non-security aware
   DNS servers in some cases.

   The extensions provide for the storage of authenticated public keys
   in the DNS. This storage of keys can support general public key
   distribution services as well as DNS security. The stored keys
   enable security aware resolvers to learn the authenticating key of
   zones in addition to those for which they are initially configured.
   Keys associated with DNS names can be retrieved to support other
   protocols. Provision is made for a variety of key types and
   algorithms.

   In addition, the security extensions provide for the optional
   authentication of DNS protocol transactions and requests.

   This document incorporates feedback on RFC 2065 from early
   implementers and potential users.

Acknowledgments

   The significant contributions and suggestions of the following
   persons (in alphabetic order) to DNS security are gratefully
   acknowledged:

      James M. Galvin
      John Gilmore
      Olafur Gudmundsson
      Charlie Kaufman
      Edward Lewis
      Thomas Narten
      Radia J. Perlman
      Jeffrey I. Schiller
      Steven (Xunhua) Wang
      Brian Wellington

Table of Contents

1. Overview of Contents

   This document standardizes extensions of the Domain Name System (DNS)
   protocol to support DNS security and public key distribution. It
   assumes that the reader is familiar with the Domain Name System,
   particularly as described in RFCs 1033, 1034, 1035 and later RFCs. An
   earlier version of these extensions appears in RFC 2065. This
   replacement for that RFC incorporates early implementation experience
   and requests from potential users.

   Section 2 provides an overview of the extensions and the key
   distribution, data origin authentication, and transaction and request
   security they provide.

   Section 3 discusses the KEY resource record, its structure, and use
   in DNS responses. These resource records represent the public keys
   of entities named in the DNS and are used for key distribution.

   Section 4 discusses the SIG digital signature resource record, its
   structure, and use in DNS responses. These resource records are used
   to authenticate other resource records in the DNS and optionally to
   authenticate DNS transactions and requests.

   Section 5 discusses the NXT resource record (RR) and its use in DNS
   responses including full and incremental zone transfers. The NXT RR
   permits authenticated denial of the existence of a name or of an RR
   type for an existing name.

   Section 6 discusses how a resolver can be configured with a starting
   key or keys and proceed to securely resolve DNS requests.
   Interactions between resolvers and servers are discussed for various
   combinations of security aware and security non-aware. Two
   additional DNS header bits are defined for signaling between
   resolvers and servers.

   Section 7 describes the ASCII representation of the security resource
   records for use in master files and elsewhere.

   Section 8 defines the canonical form and order of RRs for DNS
   security purposes.

   Section 9 defines levels of conformance for resolvers and servers.

   Section 10 provides a few paragraphs on overall security
   considerations.

   Section 11 specified IANA considerations for allocation of additional
   values of paramters defined in this document.

Appendix A gives details of base 64 encoding which is used in the
file representation of some RRs defined in this document.

Appendix B summarizes changes between this memo and RFC 2065.

Appendix C specified how to calculate the simple checksum used as a
key tag in most SIG RRs.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

2. Overview of the DNS Extensions

The Domain Name System (DNS) protocol security extensions provide
three distinct services: key distribution as described in Section 2.2
below, data origin authentication as described in Section 2.3 below,
and transaction and request authentication, described in Section 2.4
below.

Special considerations related to "time to live", CNAMEs, and
delegation points are also discussed in Section 2.3.

2.1 Services Not Provided

It is part of the design philosophy of the DNS that the data in it is
public and that the DNS gives the same answers to all inquirers.
Following this philosophy, no attempt has been made to include any
sort of access control lists or other means to differentiate
inquirers.

No effort has been made to provide for any confidentiality for
queries or responses. (This service may be available via IPSEC [RFC
2401], TLS, or other security protocols.)

Protection is not provided against denial of service.

2.2 Key Distribution

A resource record format is defined to associate keys with DNS names.
This permits the DNS to be used as a public key distribution
mechanism in support of DNS security itself and other protocols.

The syntax of a KEY resource record (RR) is described in Section 3.
It includes an algorithm identifier, the actual public key
parameter(s), and a variety of flags including those indicating the
type of entity the key is associated with and/or asserting that there
is no key associated with that entity.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

fastcase
Smarter legal research.