Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: April 2, 2016

W. Krecicki
Internet Systems Consortium

September 30, 2015

Stateless DNS Encryption
draft-krecicki-dnsenc-00

Abstract

The DNS is the last common Internet protocol that has no encryption scheme and therefore provides no privacy to the users. This document proposes an extensible mechanism providing encryption of DNS queries and responses with method for secure retrieval and verification of validity of encryption keys. It is independent of the underlying transport protocol.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 2, 2016.

Copyright Notice

Table of Contents

1. Introduction

The Domain Name System protocol is specified in RFC 1034 [RFC1034] and RFC 1035" [RFC1035]. DNS messages are unencrypted and therefore prone to eavesdropping. Although it's considered only metadata, the are a lot of data that can be leaked - from simply domain names of visited sites, to eg phone numbers (RFC 3761 [RFC3761]) or e-mail addresses (draft-ietf-dane-smime-08 [I-D.ietf-dane-smime]).

The DNS protocol is very lightweight - the queries are usually < 100 bytes long, the responses are usually < 1000 bytes (with DNSSEC). Existing transport encryption schemes such as TLS for TCP or DTLS for UDP give huge and unnecessary overhead both in amount of data sent and retrieved and in number of packets exchanged between client and server.

In DNSENC the query is encrypted using asymmetric cryptography with a securely retrieved key, the response is encrypted using symmetric encryption using one-time key provided with query. DNSENC protocol is confined within DNS and does not requires any additional external mechanism such as external PKI/CA system.

The DNSENC communication can be split into three phases:

- first the client retrieves public key for server that is stored in DNS and DNSSEC signed (this key can be cached)
- client creates the query, adds a random response encryption key and encrypts the query with servers public key
- server decrypts the message, prepares the response and encrypts it with the key provided by client

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. Communication process

To communicate securely with server, client first needs to retrieve servers public key for assymetric encryption. This key is stored in DNSEK record for reverse DNS record IP address of DNS server, as described in RFC3152, 1033, 2317. This record MUST be DNSSEC signed.

TODO alternative method - DNSEK kept by NS record

Each DNSEK RR consist of priority field, key identifier, query encryption scheme (asymmetrical, eg. RSA), query key data and possible response encryption schemes. The server might provide multiple RR records, it's client responsibility to choose a RRR that has query and response encryption schemes supported by client and has highest priority.

After choosin encryption scheme client generates a random response encryption key (symmetrical, eg. AES), prepares a regular DNS query with DNSEK record containing the response encryption scheme and key in ADDITIONAL section. This message is encrypted using query encryption key and packed, along with encryption key ID, in a DNSENC RR. A new query is created with query id copied from the encrypted message, empty QUESTION (TODO or put something there?), ANSWER and AUTHORITY sections and with DNSENC RR in ADDITIONAL section and sent to server. The response encryption key is stored along its identifier for decryption.

After receiving the query with DNSENC RR in ADDITIONAL section the server checks if it has proper key and decrypts the message. A regular DNS response packet is created, it is encrypted using response encryption key sent by client and stored along with response encryption key ID in DNSENC RR. New response packet with query ID copied from the encrypted one is created with empty QUESTION, ANSWER (TODO?) and AUTHORITY sections and with DNSENC RR in ADDITIONAL section. This response packet is sent to the client.

3. Security Considerations

The security of this protocol is based deeply on DNSSEC [RFC4033]. Protection agains downgrade attack requires wide adoption of DNSSEC.

4. References

4.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <http://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

4.2. Informative References

[I-D.ietf-dane-smime] Hoffman, P. and J. Schlyter, "Using Secure DNS to Associate Certificates with Domain Names For S/MIME", draft-ietf-dane-smime-08 (work in progress), February 2015.

[RFC3761] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, DOI 10.17487/RFC3761, April 2004, <http://www.rfc-editor.org/info/rfc3761>.

Appendix A. Additional Stuff

This becomes an Appendix.

Author's Address

Witold Krecicki
Internet Systems Consortium
Warsaw
PL

Phone: +48 502117580
Email: wpk@isc.org