INTERNET-DRAFT
DANE Working Group
Intended status: Proposed Standard
Expires: December 31, 2014
Updates: 6698 (if approved)

J. Gilmore
Electronic Frontier Foundation

July 3, 2014

Authenticating Raw Public Keys with DANE TLSA

draft-ietf-dane-rawkeys-00

Abstract

This document standardizes how the Domain Name System can authenticate Raw Public Keys. Transport Level Security now has the option to use Raw Public Keys, but they require some form of external authentication. The document updates RFC 6698 to allow the Domain Name System to standardize the authentication of more types of keying material.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents

(http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1 Background and Introduction

The Internet uses many kinds of encryption, and many kinds of keying material. These keys are authenticated in an attempt to prove that the public keys used in communication are the correct keys needed to interact with a particular server or client across the Internet.

The Domain Name System (DNS) [RFC1034, RFC1035] provides a globally distributed database for brief information about names used in the Internet. The DNS Security Extensions (DNSSEC) [RFC4033, RFC4034, RFC4035] provide authentication for this database, proving whether the information in the DNS was truly published by the owner of the associated domain name.

Transport Level Security (TLS) [RFC5246] and Datagram TLS (DTLS) [RFC6347] define a protocol that protects an Internet datastream or a series of datagrams from eavesdropping and modification. They initially used certificates in PKIX [RFC 5280] formats to store their keying material, and authenticated them via a series of trust anchors embedded in client applications.

Domain name system Authentication of Named Entities (DANE) provides a way to store application level public keys in the DNS and authenticate them using DNSSEC. The DANE TLS Authentication (TLSA) resource record [RFC6698] initially provided authentication for the PKIX certificates used in TLS and DTLS.

1.1 Summary of Changes

This document extends TLSA records to be able to authenticate more kinds of keying material than PKIX certificates. Protocols can then use their keying material with DANE by standardizing new forms of TLSA records.

As a first example of such a new form, this document extends DANE to provide authentication for Raw Public Keys. Raw Public Keys are used in place of PKIX certificates in an extension to TLS and DTLS [RFC7250]. Client applications using Raw Public Keys with TLS or DTLS can use DNSSEC to prove whether those public keys were truly published by the owner of the domain name whose server they are

accessing.

1.2 Terminology

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 Extending TLSA records to support non-PKIX keying material

This document relaxes the restriction that TLSA records can only authenticate PKIX certificates (RFC 6698, section 1.3). The DANE protocol and TLSA records can now apply to encryption keying material in general. This protocol and record type continue to apply to PKIX [RFC5280] certificates, but new standards are free to define non-PKIX keying material formats.

Wherever the term "certificate" is used in RFC 6698 to refer to fields in the TLSA record, this document extends it to refer more generally to "keying material". Thus the "certificate usage" field can be thought of as a "keying material usage" field, the "certificate association data" can now be used as "keying material association data", etc.

In addition, this document relaxes the requirement that certificate usage value 3 can only be used for PKIX format certificates (RFC 6698, section 2.1.1). Certificate usage 3 can now be used with any standardized keying material format. Certificate usages 0, 1 and 2 remain restricted to apply only to PKIX-formatted certificates in DER encoding [X.690].

3 Supporting Raw Public Keys in TLSA records

This document extends the DANE TLSA record definition to allow TLSA records to describe raw public keys as well as PKIX certificates. This extension does not define any new field values; it merely defines how existing fields are processed when being used with raw public keys, such as those provided by TLS and DTLS servers.

There are two different ways to use raw public keys in TLSA records. One is to store the public key itself, so that it can be accessed directly from the DNS. The second is to store a hash of the public key, so that a public key obtained in some other way can be authenticated via the DNS. These cases are distinguished by the matching type field in the TLSA record.

When a raw public key is to be stored in a TLSA record, the record MUST specify a certificate usage / keying material usage of 3

(domain-provided), a selector of 1 (SubjectPublicKeyInfo), and a matching type of 0. The SubjectPublicKeyInfo structure that holds the public key is placed in the certificate association / keying material association data field.

This SubjectPublicKeyInfo structure MUST be encoded in DER encoding [X.660] of Abstract Syntax Notation One (ASN.1) [X.208]. It is identical to the SubjectPublicKeyInfo structure that is described in RFC 3279 [RFC3279], which is a used as a component of PKIX certificates. It is identical to the SubjectPublicKeyInfo structure that is used in TLSA records that use a selector value of 1 and a matching type of 0 to match PKIX certificates. It contains an algorithm identifier, any optional parameters needed with that algorithm identifier, and the public key itself.

When a raw public key (that was obtained in some other way, such as in a TLS or DTLS transaction) is to be merely matched by a TLSA record, matching type 0 MAY be used, or matching types other than 0 MAY also be used, by placing the hash value of the SubjectPublicKeyInfo structure into the certificate association / keying material association data.

This document extends the meaning of the certificate usage / keying material usage value of 3 (from RFC 6699 section 2.1.1) by defining how the TLSA record is used by a client communicating with a TLS or DTLS server that uses raw public keys. This extension adds to, rather than replacing, the definition of certificate usage 3 with TLS or DTLS servers that use PKIX certificates.

> 3 -- Keying material usage 3 is also used to specify a raw public key that MUST match the raw public key presented by the server in TLS or DTLS. When the server provides a raw public key, there is no PKIX certificate and no PKIX validation is done. The server's raw public key MUST match the raw public key provided in the TLSA record. This keying material usage is sometimes referred to as "domain-issued" because it allows a domain administrator to directly certify a domain's public keys.

4 Security Considerations

The encoding used in the TLSA resource record for Raw Public Keys is identical to the encoding used to match the public key of a PKIX certificate. This allows a single TLSA record to match both a PKIX certificate used in traditional TLS or DTLS, and to also match a Raw Public Key provided in extended TLS or DTLS. This offers TLS or DTLS servers an easy way to interoperate with both traditional and extended clients. They can use the same public and private key when communicating with either extended or traditional clients.

Since TLSA records use a protocol type and port number as a prefix on the domain name, services that use Raw Public Keys on various ports accessed through the same domain name are free to use different keying material. Using diverse keying material for different services can improve the robustness of the services after a key compromise. For example, email service on port 25 can continue with full security, even after the private key protecting HTTPS service on port 443 has been compromised. This is a tighter binding between public keys and services than that provided by PKIX certificates, which do not distinguish port numbers. When PKIX certificates are authenticated with TLSA usages 0, 1, or 2, a PKIX certificate that was originally used with HTTPS could be used for a man-in-the-middle attack on email service as well, after its corresponding private key has been compromised. This cross-port attack does not work when the domain name uses TLSA usage 3 to authenticate different Raw Public Keys (or PKIX certificates) for the different services on different ports.

In the TLS and DTLS protocol, certificate types are often negotiated before the relevant TLSA records are available to the client. Server operators who anticipate using TLSA records to authenticate the server should always ensure that if their server offers support for Raw Public Keys, then their server's domain name(s) SHOULD contain TLSA records that match the public key that the server offers. Failure to publish such TLSA records would otherwise lead to an authentication failure in clients that opt to use Raw Public Keys, even if TLSA records exist that authenticate PKIX certificates with usages 0, 1, or 2. This is not an issue when Raw Public Keys are used with out-of-band non-DANE authentication.

When using Raw Public Keys and TLSA records, the security of the domain name system records directly affects the security of the communications protected by TLS or DTLS. If the domain's DNS records are compromised, or the DNS records that delegate name service to this domain are compromised, communications can be blocked, redirected, intercepted, or modified. The DANE TLSA Security Considerations section [RFC6698] provides further details.

5 IANA Considerations

In the IANA "TLSA Certificate Usages" registry created by Section 7.2 of RFC 6698, the value "3" ("Domain-issued certificate") should have its short description changed to "Domain-issued keying material", and should have this document added as a reference document.

6 References

6.1 Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3279] Polk, T., Housley, R., Bassham, L, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, April 2002.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6698] Hoffman, P., Schylter, J., "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

[RFC7250] Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., Kivinen, T., "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, May 2014

[X.208] CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988.

[X.690] "Recommendation ITU-T X.690 (2002) | ISO/IEC 8825-1:2002, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules

(DER)", July 2002.

6.2 Informative References

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

Authors' Addresses

John Gilmore
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94117
United States

EMail: gnu@ietf.toad.com