Network Working Group
Internet-Draft
Intended status: Experimental
Expires: January 23, 2015

D. Zhang
Huawei

July 22, 2014

Certificate Transparency for Domain Name System Security Extensions
draft-zhang-ct-dnssec-trans-00

Abstract

In draft-ietf-trans-rfc6962-bis, a solution is proposed for publicly logging the existence of Transport Layer Security (TLS) certificates using Merkle Hash Trees. This document tries to use this idea in DNSSEC and publicly logging the existence of keys used in securing DNS resource records.

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].

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 January 23, 2015.

Table of Contents

1. Introduction

[I-D.ietf-trans-rfc6962-bis] specifies a Certificate Transparency (CT) mechanism to disclosing TLS certificates into public logs so as to benefit the public to monitor the operations in issuing certificates. The logs do not prevent mis-issuing behavior, but the provided public audibility can increase the possibility in detecting certain mis-behaviors of issuers. The logs are constructed with Merkle Hash Trees to ensure the append-only property, and thus enable anyone to verify the correctness of each log and to monitor when new certificates are added to it. Note that CT is a common mechanism although [I-D.ietf-trans-rfc6962-bis] only describe its usage in publishing TLS server certificates issued by public certificate authorities (CAs).

This document discusses the application of CT to publicly logging the public keys used by DNSSEC. DNSSEC distributes public keys to provide origin authentication and integrity protection for DNS resource records. In order to prove the validity of keys used for

signing DNS data, DNSSEC uses DNS public key (DNSKEY) RRsets and Delegation Signer (DS) RRsets to form authentication chains for the signed data, with each link in the chains vouching for the next. If an authentication chain can be eventually connected to the a trsuted public key, the client can then ensure the key for signing the data is valid.

The application of CT to publish the existence of (DNSKEY) RRsets and (DS) RRsets can benefit the detection of misissurance of DNSSEC keys. For instance, if the owner of foo.example.com finds that its parent zone (example.com) publish a DS RR for its zone which however does not point to any legal zone signing keys or key signing keys, the owner can claim that a mississuance event occures.

This work re-use some text in [I-D.ietf-trans-rfc6962-bis].

2. Cryptographic Components of Certificate Transparency

The introduce of cryptographic components of CT is in Section 2 of [I-D.ietf-trans-rfc6962-bis]. When applying CT for NDSSEC, a log is a single, ever-growing, append-only Merkle Tree of DNSKEY and DS RRs.

3. Log Format and Operation

When generating a new DNSKEY RR or a DS RR (i.e., during the publication of a KSK or a zone authentication key), a zone owner will publish the RR to the CT logs. Because a key will not be trusted by clients unless logged, it is expected that a zone owner will usually deliver the RRs (keys) for audit purposes.

Identical to what is specified in [I-D.ietf-trans-rfc6962-bis],when a valid DNSKEY RR or a valid DS RR is submitted to a log, the log MUST immediately return a Signed Certificate Timestamp (SCT). The SCT is the log's promise to incorporate the RR in the Merkle Tree within a fixed amount of time known as the Maximum Merge Delay (MMD). If the log has previously seen the certificate, it MAY return the same SCT as it returned before. DNS servers MUST provide an SCT from one or more logs to the client within a SCT RR. DNS clients MUST NOT trust a key that does not have a valid SCT.

3.1. Log Entries

A zone owner can submit a DNSKEY or DS RR to any log before publishing the RR. In order to enable attribution of each logged RR to its issuer, the log SHALL publish a list of acceptable zone signing public keys (or hashes of public keys) of root zones or islands of security. Each submitted RR MUST be accompanied by all additional RRs (DNSKEY RRs, DS RRs, and RRSIG RRs) which construct an

authentication chain to an accepted root public key. Note that the NSEC RR is not provided since the existence of this type of RR indicates the broken of an authentication chain.

A typical authentication chain is Public Key->[DS->(DNSKEY)*->DNSKEY]*->RRset, where "*" denotes zero or more subchains. (DNSKEY)* indicates that DNSSEC permits additional layers of DNSKEY RRs signing other DNSKEY RRs within a zone. Each DNSKEY/DS RR in the chain is authenticated by a RRSIG RR. In practice, a RRSIG RR may be used to sign a DS/DNSKEY RRset rather than a single RR. In this case, not only the DS/DNSKEY RR on the authentication chain but also other records in the RRset SHOULD be provided to the log the verification purpose. Otherwise, the log may have to consult DNS again in order to verify the authentication chains.

4. Including the Signed Certificate Timestamp into DNS Security Extensions

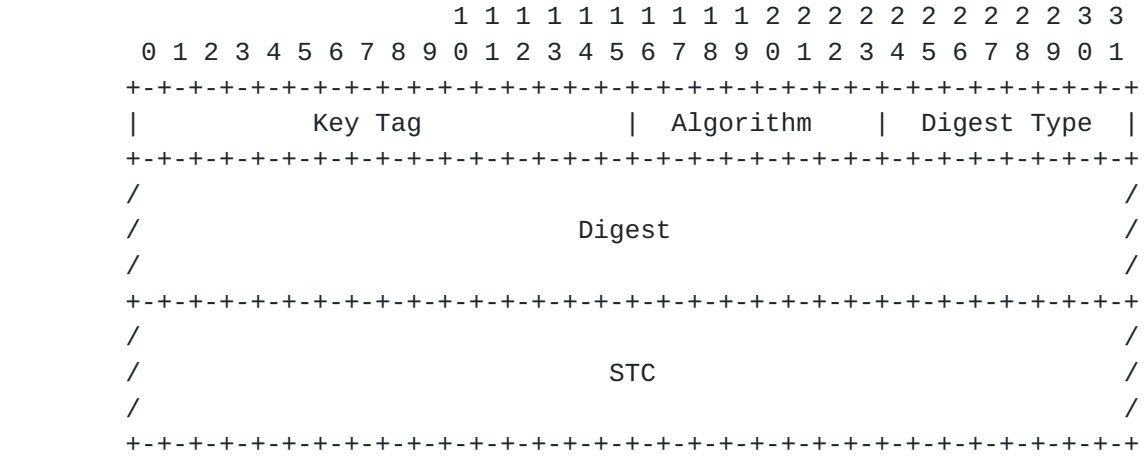
4.1. SCT RR

The SCT associated with a DNSKEY/ DS RR is stored within a STC RR.

The type number for the DS record is TBD1.

The DS resource record is class independent.

The DS RR has no special TTL requirements.



4.1.1. The Key Tag Field

The Key Tag field lists the key tag of the DNSKEY RR referred to by the SCT record, in network byte order. Appendix B of [RFC4034] describes how to compute a Key Tag.

4.1.2. The Algorithm Field

The Algorithm field lists the algorithm number of the DNSKEY RR referred to by the SCT record. Appendix A.1 of [RFC4034] lists the algorithm number types.

4.1.3. The Digest Type Field

The Digest Type field identifies the algorithm used to construct the digest used to identify the DNSKEY RR that the SCT RR refers to. Appendix A.2 of [RFC4034] lists the possible digest algorithm types.

4.1.4. The Digest Field

The method of calculating digest is identical to what is specified in Section 5.1.4 of [RFC4034]

4.1.5. The SCT Field

This field contains the SCT got from the log.

4.2. Operations

After introducing the SCT RR, the verification procedures of DNS data specified in DNSSEC[RFC4305] do not change a lot. However, the correctness of CTS needs to be assessed during checking the validity of a NDSKEY/DS RR.

A NDSKEY/DS RR needs to be associated with a CTS RR which contains a valid CTS and signed with a proper public key. Otherwise, the NDSKEY/DS RR will not be used to construct the authentication chain. The signatures of NDSKEY/DS RR and its CTS RR should be stored in different RRSIG RR respectively. In addition, a DNS server will sends CTS RRs and the associated RRSIG RRs to a resolver only when it indicates the support of CT in the request.

5. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

6. Security Considerations

6.1. Logging other types of RRs

The above section tries to propose a solution to disclose keys for DNSSEC in logs for the public to audit. However, it may be valuable to also log the RRs specified in [RFC1035]. For instance, assume there is an attacker which has compromised the zone authentication key and is able to perform the MITM attack between a resolver and the DNS server of the zone. It is possible for an attacker to transfer a forged RR which is signed with the compromised key. The current solution cannot benefit the detection of this attack in this scenario. However, if the RR is also required to be uploaded to public logs, the condition is changed. If the attacker does not publish the RR to a log, it cannot get the SCT. When the attacker tries to publish the RR to the log, the owner of the zone may detect the problem even if the attacker can provide keys to convince the log to accept the RR.

7. Acknowledgements

8. Normative References

[I-D.ietf-trans-rfc6962-bis]
Laurie, B., Langley, A., Kasper, E., and R. Stradling, "Certificate Transparency", draft-ietf-trans-rfc6962-bis-04 (work in progress), July 2014.

[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.

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

[RFC4305] Eastlake, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, December 2005.

Author's Address

Dacheng Zhang
Huawei

Email: zhangdacheng@huawei.com