DNS Publication of HTTP Strict Security and Key Pinning Declarations

DNS Publication HSTS & HPKP

<ietf>draft-hallambaker-webseccaa

<version>00

<ipr>trust200902

<area>sec

<publisher>Internet Engineering Task Force (IETF)

<status>Standards Track

<category>Standards Track

<author>Phillip Hallam-Baker

<fullname>Phillip

<initials>P. M.

<organization>Comodo Group Inc.

<surname> Hallam-Baker

<email>philliph@comodo.com

<keyword>CAA

<keyword>X.509

<keyword>PKIX

<keyword>Pinning

Abstract

HTTP Strict Transport Security (HSTS) and Public Key Pinning (HPKP) define security policies that provide Secure After First Use security when published through HTTP over TLS. This specification defines a mechanism allowing HSTS and HPKP assertions to be published using DNS CAA records to support Secure On First Use mechanisms.

Definitions

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].

Introduction

HTTP Strict Transport Security (HSTS) [!RFC6797] defines a mechanism enabling web sites to declare themselves accessible only via secure connections and/or for users to be able to direct their user agent(s) to interact with given sites only over secure connections. An HTTP host declares itself an HSTS Host by issuing to UAs an HSTS Policy, which is represented by and conveyed via the Strict-Transport-Security HTTP response header field over secure transport (e.g., TLS).

While signaling the security configuration of the HTTP server in-band affords considerable deployment advantages, the security policy enforcement is of the ‘Secure After First Contact’ type. Conveying HSTS policy declarations inband does not and cannot provide security on first contact.

One response to this limitation is the use of ‘pre-loaded list’ registries as described in [!RFC6797] section 14.6. Such lists are frequently employed by HTTP clients supporting the HTTP Strict Security mechanism.

The Certificate Authority Authorization record (CAA) [!RFC6844] provides an extensible mechanism for publishing assertions that relate to the issue and use of PKIX certificates. This document defines CAA tags for HTTP Strict Security (HSTS) and Public Key Pinning (HPKP).

Unlike TLSA record specified by DANE [~RFC6698], the syntax and intended semantics of a HSTS or HPKP record are identical to the corresponding HTTP headers. This affords considerable convenience in provisioning as all that is necessary is to forward data from the HTTP headers to the DNS service, a task which may be performed with little or no code.

# Record Format and Interpretation

The CAA record is an extensible DNS Resource Record defined for the purpose of making assertions about CA issued PKIX keys in the DNS.

Although the intended semantics are identical, the context is not. In particular, a CAA record is presented through the DNS rather than in-band within the TLS protocol. While a CAA record MAY be authenticated by a valid DNSSEC signature, such a signature only establishes that the record is authoritative, it does not provide evidence of the state of the TLS server to which the record refers.

The consequences of the difference in semantics are discussed in the security considerations section.

## Record Format

The CAA record has four fields:

* A flags field, permitting a criticality bit to be set.
* A tag length field specifying the length of the following tag value
* An attribute tag. Reserved tag values are specified in the IANA "Certification Authority Restriction Properties" registry.
* A data block specifying the value.

### HSTS

To publish a HTTP Strict Security declaration as a CAA record, the following parameters are used:

* Flags = 0
* Tag Length = 4
* Tag = 'hsts'
* Value = The HTTP Strict Security policy declaration as specified in [!RFC6797].

### HPKP

To publish a Public Key Pinning declaration as a CAA record, the following parameters are used:

* Flags = 0
* Tag Length = 4
* Tag = 'hpkp'
* Value = The Public Key Pinning policy declaration as specified in [!I-D.ietf-websec-key-pinning].

## Interpretation

A CAA record with a hsts or hpkp tag is an assertion that HTTPS queries to the specified domain will return the data specified in the Value section as a HTTP Strict-Transport-Security header or Public Key Pinning header.

While the semantics of data presented through a CAA record are identical to the presentation of the same record through a HTTP header by a Web server operating on port 443 of the same domain, the context in which the record is presented are different. In particular, DNS records have an explicit expiry time while HTTP transactions do not.

Security Considerations

HSTS and HPKP are security policy mechanisms that attempt to set a minimum level of security. Providing additional channels through which security policy can be published does not introduce new security vulnerabilities affecting confidentiality or integrity but does create new opportunities for denial of service. In particular, self-inflicted denial of service attacks.

As noted previously, CAA records provide an out-of-band mechanism for publication of HSTS and HPKP. Since the records are not presented by the

CAA records with the hsts or hpkp tag MUST NOT be cached for longer than the DNS expiry interval.

When used to compile pre-loaded lists, hsts and hpkp declarations published by CAA records SHOULD be validated by an attempt to establish a HTTP connection over TLs if possible and verifying that the HTTP headers presented in the response are consistent. If this is not possible (e.g. the Web site is not publicly visible), the list compiler SHOULD re-verify the published CAA records on a regular basis.

IANA Considerations

On publication, IANA should add the following entries to the "Certification Authority Restriction Properties" registry:

Tag Meaning Reference

----------- -------------------------------------- ---------

hsts Strict-Transport-Security [This]

hpkp Public-Key-Pins [This]

issue Authorization Entry by Domain [RFC6844]

Acknowledgements

TBS