Internet Engineering Task Force	P. Hallam-Baker
Internet-Draft	Comodo Group Inc.
Intended status: Standards Track	R. Stradling
Expires: April 25, 2012	Comodo CA Ltd.
	October 23, 2011

TOC

Security Policy Distribution Format (SPDF) draft-hallambaker-securitypolicy-00

Abstract

This document describes a format for distributing security policy statments.

Individual security policy statements are expressed in a HTTP compatible header syntax. Lists of security policy statements are exchanged as signed CMS objects. Strong references to static data objects are formed using Named Information (ni) URI specifiers.

Status of this Memo

Copyright Notice

Table of Contents

1. Definitions

TOC

1.1. Requirements Language

TOC

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]**

1.2. Defined Terms

TOC

The following terms are used in this document:

Certificate
An X.509 Certificate, as specified in **RFC 5280** [RFC5280].

Certification Policy (CP)
Specifies the criteria that a Certification Authority undertakes to meet in its issue of certificates.

Certification Practices Statement (CPS)
Specifies the means by which the criteria of the Certification Policy are met. In most cases this will be the document against which the operations of the Certification Authority are audited.

Certification Authority (CA)
An entity that issues Certificates in accordance with a specified Certification Policy.

Domain
The set of resources associated with a DNS Domain Name.

Domain Name
A DNS Domain name as specified in **RFC 1035** [RFC1035] and revisions.

Domain Name System (DNS)

The Internet naming system specified in **RFC 1035** [RFC1035] and revisions.

DNS Security (DNSSEC)

Extensions to the DNS that provide authentication services as specified in **RFC 4033** [RFC4033] and revisions.

Public Key Infrastructure X.509 (PKIX)

Standards and specifications issued by the IETF that apply the **X.509** [X.509] certificate standards specified by the ITU to Internet applications as specified in **RFC 5280** [RFC5280] and related documents.

Resource Record (RR)

A set of attributes bound to a Domain Name.

Relying Party

A party that makes use of an application whose operation depends on use of a Certificate for making a security decision.

Relying Application

An application whose operation depends on use of a Certificate for making a security decision.

TOC

2. Introduction

Recent compromises of critical infrastructure have highlighted the weaknesses that result from the fact that on the Internet, security is an option, not the default.

Security Policy provides a mechanism for advising parties of the minimum degree of security that they should accept for a communication and thus preventing downgrade attacks.

TOC

2.1. Requirements

Security Policy statements provide a mechanism for advising parties of the risk of a downgrade attack and the enforcement actions that are appropriate based on the quality of the security policy information available.

While the natural inclination of security specialists is to advise that a security policy violation always result in a hard failure with the corresponding transaction being aborted, this approach imposes a high cost for false positives. Previous attempts to employ security policy data (e.g. in DKIM) have faced objections from those fearing that the false positive rate will be unacceptably high.

Recent events have demonstrated that the value of reporting a security policy violation is considerably higher than than security policy enforcement on a limited scale. While security policy enforcement has the potential to protect the individual Internet user, reporting a violation to the appropriate parties has the potential to protect the entire community of Internet users.

TOC

2.1.1. Protocol Downgrade Attack

In a protocol downgrade attack the attacker causes client software to communicate en-clair when TLS or some other security enhancement is offered.

TOC

2.1.2. CA Downgrade Attack

In a CA downgrade attack the attacker applies for a certificate from a different issuer to that authorized by the Domain name holder or for a category of certificate with lest strict validation requirements.

TOC

2.1.3. Use of Revoked Certificate

Although PKIX specifies two mechanisms for certificate status checking, many clients will accept certificates when access to the certificate status checking infrastructure fails.

TOC

2.1.3.1. Use of Expired Certificate

Although use of expired certificates is discouraged, the frequency with which use of expired certificates occurs from administrative oversight prevents strict enforcement.

TOC

2.1.4. Security Policy Origination

Security policy statements may be obtained from explicit statements by domain name holders or obtained heuristically from observation of the network.

TOC

2.1.4.1. Explicit

A domain name holder MAY specify security policy explicitly through publication mechanisms that include:

> Publishing statements in Security Policy Distribution Format
>
> Security Policy Statements in HTTP headers
>
> Security Policy Statements in DNS records
>
> Out of band contact with remediation parties.
>
> Statements to a Certification Authority at certificate issue.

Even though a statement is explicit, an enforcement point may only learn of its existence through heuristic means. For example observing DNS traffic, use of Web crawlers and HTTPS inspection.

Publication of an explicit Security policy Statement requires a considerable commitment of time and effort for a large site.

TOC

2.1.4.2. Heuristic

Security policy data MAY also be determined heuristically by observation of network traffic. If a site has been using a particular CA for many years and a certificate is suddenly detected from an obscure issuer, questions may be asked.

While the quality of heuristic data may fall short of that required to abort transactions by itself, it can still provide a useful basis for reporting potential violations and for enforcement when combined with data from other sources.

TOC

2.1.5. Security Policy Distribution

Security policy can be distributed through multiple channels. The best choice of channel depends on the information in question and the application.

TOC

TOC

2.1.5.1. Embedded

The Security Policy is embedded in client or operating system code. This approach has traditionally been limited to embedding revocation notices for certificates that have been known to be fraudulently issued.

TOC

2.1.5.2. In-Band

The security policy data is carried in the protocol to which the policy applies. E.G HTTP headers for a HTTP transaction. One drawback to this approach is that it only provides 'secure after first contact'.

TOC

2.1.5.3. DNS

The DNS has been used to distribute Security Policy Statements. The principle drawback being that deployment of DNSSEC is immature and likely to be blocked in the regions where security policy is most needed.

TOC

2.1.5.4. Data Driven Update

The format described in this document is designed to support data driven update.

The main limitation to this approach is that it does not scale. Thus the use of the distribution format should be limited to distributing policy for the domains that carry the highest risk.

TOC

2.1.5.5. Irregular

Security Policy distribution is hard because the adversaries encountered to date include nation state actors with complete control of the local network infrastructure. It is thus not possible to address every possible need in a standard based approach since the adversary can block deployment of the necessary standards.

It follows that standards based techniques SHOULD be supplemented by resort to irregular methods where necessary.

TOC

2.2. Security Policy Statements

TOC

2.2.1. Common Syntax

All Security Policy Statements have a common syntax based on the syntax used in HTTP and SMTP message format.

Forgetting about the traditional white space and line wrapping considerations, the syntax has the format has the following common syntax:

```
statement         = token ":"  values

values            = principal-value *("," principal-value)
                                        *( ";" parameter )
```

```
principal-value   = dns-name | uri | quoted-string

parameter         = attribute "=" value
attribute         = token
value             = token | quoted-string

WS                = " " | tab
```

TOC

2.2.2. Common Parameters

The following parameters MAY occur in any Security Policy Statement.

TOC

2.2.2.1. Domain=<dns-name>

The domain(s) to which the security policy statement applies.

The wildcard character '*' MAY be used to indicate that the security policy statement also applies to subdomains within the specified domain.

To facilitate mapping of security policy originated in DNS records, the rules for use of wildcards are the same as those defined for DNSSEC. I.e. wildcards SHALL only occur as the first label in a DNS name, if a domain is in the scope of multiple security policy statements, the principle of closest match is applied.

TOC

2.2.2.2. Protocol=<Protocol>*

A list of protocols to which the Security Policy applies. Protocols are identified by their SRV prefix labels.

TOC

2.2.2.3. UTC=<date-time>

The time at which the security policy statement was obtained. This MAY be earlier than the time at which the SPDF document is signed but SHOULD NOT be later.

TOC

2.2.2.4. Expire=<date-time>

The time at which the security policy statement expires. This MUST NOT be earlier than the time at which the SPDF document was signed.

TOC

2.2.3. Statement: CA-PIN: <uri>

The CA-PIN statement is used to prevent a certificate issuer downgrade attack. A certificate SHALL be in violation of the specified security policy if the domain in question was within the scope of at least one CA-PIN statement at the time in question and the certificate does not comply with the requirements of any CA-PIN statements that were active at the time in question.

The principal parameter of a CA-PIN statement is an ni URI that specifies the criteria for the pinning.

TOC

2.2.3.1. Match= 'key' | 'csk' | 'cert' | 'path'

Specifies whether the specified Named Information URI applies to an end entity subject key (key), a certificate signing subject key (csk), an end entity certificate (cert) or a certificate signing certificate (path). If no match is specified, the 'key' match is the default.

TOC

2.2.3.1.1. Calculating the digest of a Subject Key.

TBS

TOC

2.2.3.1.2. Calculating the digest of a Certificate.

TBS

TOC

2.2.3.2. After=<date-time>

The statement is only to be applied to certificates issued after the specified date and time.

TOC

2.2.3.3. Before=<date-time>

The statement is only to be applied to certificates issued before the specified date and time.

TOC

2.2.3.4. Unpin=<uri>

A Named Information URI that specifies the digest of an unpinning value. Disclosure of the unpinning value has the effect of revoking the corresponding security policy statement to which it is attached.

The unpinning value SHOULD be a randomly chosen nonce with sufficient ergodicity to make determination by brute force attack infeasible.

TOC

2.2.4. Statement: Unpin: <data>

An unpinning value for a previously distributed CA pinning statement encoded as Base64.

TOC

2.2.5. Statement: Revoke: <uri>

The Revoke statement is used to declare that a certificate is invalid.

While the functionality of the Revoke statement overlaps the capabilities and functionality of the existing PKIX revocation schemes (CRLs and OCSP), it is intended for a different field of use.

In particular the Revoke statement SHOULD NOT be employed except as a last resort mechanism for use in situations that are not adequately addressed by the existing certificate status infrastructure and the risk of relying on the revoked certificate is unacceptably high.

TOC

2.2.6. Statement: Action: <action>

Specifies the action that SHOULD be performed in the case that a security policy violation is detected. Valid actions are 'Ignore', 'Advise', 'Fail' and 'Block':

Ignore
    The client SHOULD ignore policy violations. This option is intended for use in testing Security Policy configuration prior to requesting enforcement.

Advise
    The client SHOULD advise the user when policy violations occur but not impede access to the corresponding network resource.

Fail
    The client SHOULD advise the user that a policy violation has occurred and discourage (but not prevent) access to the corresponding network resource.

Block
    The client SHOULD advise the user that a policy violation has occurred and prevent access to the corresponding network resource.

Note that the specification of client actions is independent of reporting requests.

TOC

2.2.7. Statement: Report: <dns-name>

This part is to be aligned with whatever is agreed in PKIX for use in CAA.

TOC

2.2.8. Statement: TLS: <level>

Specifies the use of TLS:

refused
    Use of TLS is not supported.

unknown
    Use of TLS is unkown.

optional
    Use of TLS is optional.

required
    Use of TLS is required.

strict
    Use of TLS is required with Strict Transport Security.

Additional parameters MAY be specified to further control the mode of use of TLS. For example the minimum version of the protocol to be used. [[While this could be extended to include cipher suites it is believed that the existing protocol is sufficiently proofed against downgrade attack on cipher suites. If this should be found not to be the case it would likely drive an urgent update of the protocol version.]]

TOC

2.2.8.1. version=<version>

Specifies the minimum version of TLS to be used in a format that I am sure someone will advise me on.

TOC

3. Distribution Format

A SPDF document consists of a Cryptographic Message Syntax object **[RFC5652]** that contains a list of Security Policy statements. SPDF documents SHOULD be signed and MAY be encrypted.

TOC

3.1. Cryptographic Message Syntax Properties

[TBS details of CMS options that MUST be supported, crib this from SMIME]

TOC

3.2. JSON Packaging

[TBS optional, not sure if it is actually very usefull for this particular application but...]

TOC

4. Security Considerations

TBS

TOC

5. IANA Considerations

TBS

Need to create a registry for the statements and parameters.

TOC

6. Normative References

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

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

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

[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 (**TXT**).

[RFC5652] Housley, R., "**Cryptographic Message Syntax (CMS)**," STD 70, RFC 5652, September 2009 (**TXT**).

[X.509] International Telecommunication Union, "**ITU-T Recommendation X.509 (11/2008): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks**," ITU-T Recommendation X.509, November 2008.

TOC

Authors' Addresses

Phillip Hallam-Baker
Comodo Group Inc.
Email: **philliph@comodo.com**

Rob Stradling
Comodo CA Ltd.
Email: **rob.stradling@comodo.com**