Host Identity Protocol
Internet-Draft
Intended status: Informational
Expires: January 15, 2009

Heer
Distributed Systems Group, RWTH
Aachen University
Varjonen
Helsinki Institute for Information
Technology

July 14, 2008

HIP Certificates
draft-varjonen-hip-cert-01

Status of this Memo

Abstract

This document specifies a certificate parameter called CERT for the Host Identity Protocol (HIP). The CERT parameter is a container for Simple Public Key Infrastructure (SPKI) and X.509.v3 certificates. It is used for carrying these certificates in HIP control messages. Additionally, this document specifies the representations of Host Identity Tags in SPKI and X.509.v3 certificates.

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].

1. Introduction

Digital certificates bind a piece of information to a public key by means of a digital signature, and thus, enable the holder of a private key to generate cryptographically verifiable statements. The Host Identity Protocol (HIP)[RFC5201] defines a new cryptographic namespace based on asymmetric cryptography. Each host's identity is derived from a public key, allowing hosts to digitally sign data with their private key. This document specifies the CERT parameter that is used to transmit digital signatures in HIP. It corresponds to the placeholder specified in Section 2 of [RFC5201].

2. CERT Parameter

The CERT parameter is a container for a certain types of digital certificates. It may either carry SPKI certificates or X.509.v3 certificates. It does not specify any certificate semantics. However, it defines some organizational parameters that help HIP hosts to transmit semantically grouped parameters in a more systematic way.

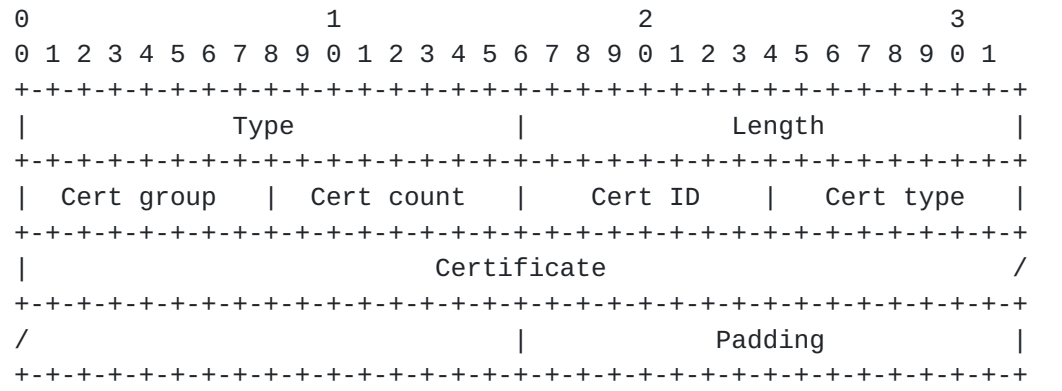
The CERT parameter may be covered by the HIP SIGNATURE field and is a non-critical parameter.

Each HIP packet may contain multiple CERT parameters. If these parameters must be handled in certain sequence, the Cert group and the Cert count field must be set. Ungrouped certificates exhibit a unique Cert group field and set the Cert count to 1. CERT parameters with the same Cert group number in the group field indicate a logical grouping. The Cert count field indicates the number of grouped CERT parameters.

CERT parameters that belong to the same CERT group may be contained in multiple sequential packets. This is indicated by a higher Cert count than the amount of CERT parameters with matching Cert group fields in a packet. Within a HIP packet, CERT parameters must be placed in ascending order according to their Cert group field. Cert groups may only span multiple packets if the Cert group does not fit the packet. Only one Cert group may span two subsequent packets.

The Cert ID acts as a sequence number to identify the certificates in a Cert group. The numbers in the Cert ID field must start from 1 up to Cert count.

The CERT parameter can be used in R1, I2, R2, UPDATE and NOTIFY messages. When CERT parameter is used in R1 message it is NOT recommended to use grouping or hash and URL encodings. Initiator and Responder can detect middleboxes on the path after R1 message is sent by checking if control packets contain ECHO_REQUEST_M parameters as defined in [HIP.middle_auth].



Type	768
Length	Length in octets, excluding Type, Length, and Padding
Cert group	Group ID grouping multiple related CERT parameters
Cert count	Total count of certificates that are sent, possibly in several consecutive HIP control packets.
Cert ID	The sequence number for this certificate
Cert Type	Describes the type of the certificate
Padding	Any Padding, if necessary, to make the TLV a multiple of 8 bytes.

The following certificate types are defined:

Cert format	Type number
SPKI	1
X.509.v3	2
Hash and URL of SPKI	3
Hash and URL of X.509.v3	4

All implementations MUST support SPKI. The next section outlines the use of HITs in SPKI. The SPKI and its formats are defined in [RFC2693]. X.509.v3 certificates are defined in [RFC3280]. Wire format for X.509.v3 is Distinguished Encoding Rules format as defined in [X.690].

Hash and URL encodings (3 and 4) are used as defined in [RFC4306]. Using hash and URL encodings results in smaller HIP control packets, but requires the receiver to resolve the URL or check local cache against the hash.

It is not recommended to use hash and URL encodings when HIP-aware middleboxes are present on the communication path between peers because fetching remote certificates requires the middlebox to buffer the packets and to request remote data. This makes these devices prone to denial of service (DoS) attacks. Moreover, middleboxes and responders that request remote certificates can be used as deflectors for distributed denial of service attacks.

3. SPKI Cert Object and Host Identities

When using SPKI certificates to transmit information related to HIP hosts, HITs need to be enclosed within the certificates. In the following we define the representation of those identifiers for SPKI given as S-expressions. Note that the S-expressions are only the human-readable representation of SPKI certificates.

As an example the Host Identity Tag of a host is expressed as follows:

```
Format:  (hash hit hit-of-host)
Example: (hash hit 2001:13:724d:f3c0:6ff0:33c2:15d8:5f50)
```

Appendix A shows a full example SPKI certificate with HIP content.

4. X.509.v3 Certificate Object and Host Identities

When using X.509.v3 certificates to transmit information related to HIP hosts, HITs need to be enclosed within the certificates. HITs are represented as issuer and subject alternative name X.509.v3 extensions as defined in [RFC2459]. Because the Distinguished Name (DN) in X.509.v3 certificate cannot be empty HITs are also placed into the Common Name (CN) in a colon delimited presentation format.

As an example the HIT of a host is expressed as follows:

```
    Format:
        Issuer: CN=hit-of-host
        Subject: CN=hit-of-host

        X509v3 extensions:
            X509v3 Issuer Alternative Name:
                IP Address:HIT-OF-HOST
            X509v3 Subject Alternative Name:
                IP Address:HIT-OF-HOST

    Example:
        Issuer: CN=2001:14:6cf:fae7:bb79:bf78:7d64:c056
        Subject: CN=2001:14:6cf:fae7:bb79:bf78:7d64:c056

        X509v3 extensions:
            X509v3 Issuer Alternative Name:
                IP Address:2001:14:6CF:FAE7:BB79:BF78:7D64:C056
            X509v3 Subject Alternative Name:
                IP Address:2001:14:6CF:FAE7:BB79:BF78:7D64:C056
```

Appendix B shows a full example X.509.v3 certificate with HIP content.

5. Revocation of Certificates

Revocation of SPKI certificates is handled as defined in Section 5. in [RFC2693] Revocation of X.509.v3 certificates is handled as defined in Section 5 in [RFC2459].

6. IANA Considerations

This document defines the CERT parameter for the Host Identity Protocol [RFC5201]. This parameter is defined in Section 2 with type 768. The parameter type number is also defined in [RFC5201]. The

Cert Group and Cert ID namespaces are managed locally by each peer that sends CERT parameters in HIP packets.

7. Security Considerations

Certificate grouping allows the certificates to be sent in multiple consecutive packets. This might allow similar attacks as IP-layer fragmentation allows, i.e. sending of fragments in wrong order and skipping some fragments to delay or stall packet processing by the victim in order to use resources (e.g. CPU or memory).

8. Acknowledgements

The authors would like to thank M. Komu and T. Henderson of fruitful conversations on the subject.

9. References

9.1. Normative References

[HIP.middle_auth] Heer, T., "End-Host Authentication for HIP Middleboxes", <draft-heer-hip-middle-auth-00.txt>.

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

[RFC2459] Housley, R., Ford, W., Polk, T., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

[RFC2693] Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and T. Ylonen, "SPKI Certificate Theory", RFC 2693, September 1999.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC5201] Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.

9.2. Informative References

[X.690] ITU-T, "Recommendation X.690 Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", July 2002, <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>.

Appendix A. SPKI certificate example

This section shows a self-signed SPKI certificate of HIT 2001:14:6cf:fae7:bb79:bf78:7d64:c056. The example has been indented for readability.

```
(sequence
  (public_key
    (rsa-pkcs1-sha1
      (e #010001#)
      (n |n1CheoELqYRSkHYMQddub2TpILl+6H9wC/as6zFCZqOY43hsZgAjG0F
          GoQwtyOyQjzO2Ykb2TmUCZemTYui/sR0zIbdwg1xafKl7ggZDkhk5an
          PtGDxJxFalTYo6/A5ZQv8uatbaJgB/G7VM8G+O9HLucadad2zQUXpQf
          gbK3S8=|
      )
    )
  )
  (cert
    (issuer
      (hash hit 2001:0014:06cf:fae7:bb79:bf78:7d64:c056)
    )
    (subject
      (hash hit 2001:0014:06cf:fae7:bb79:bf78:7d64:c056)
    )
    (not-before "2008-07-12_22:11:07")
    (not-after "2008-07-22_22:11:07")
  )
  (signature
    (hash sha1 |kfElDhagiK0Bsqtj32Gq3t/1mxgA|)
    |HiIqjjZIUzypvoxQyO0UovPm5uC4Xte0scEcBnENDIfn2DNy/bAtxGEdKq4O
     dW80vTCmkF8/HXclgXLLVch3DxRNdSbYiiks000HpQt/OKqlTH+uUHBcHOAo
     E42LmDskM9T5KQJoC/CH7871zfvojPnpkl2dUngOWv4q0r/wSJ0=|
  )
)
```

Appendix B. X.509.v3 certificate example

This section shows a self-signed X.509.v3 certificate of HIT 2001:14:6cf:fae7:bb79:bf78:7d64:c056.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=2001:14:6cf:fae7:bb79:bf78:7d64:c056
        Validity
            Not Before: Jul 12 18:58:38 2008 GMT
            Not After : Jul 22 18:58:38 2008 GMT
        Subject: CN=2001:14:6cf:fae7:bb79:bf78:7d64:c056
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:9f:50:a1:7a:81:0b:a9:84:52:90:76:0c:41:d7:
                    6e:6f:64:e9:20:b9:7e:e8:7f:70:0b:f6:ac:eb:31:
                    42:66:a3:98:e3:78:6c:66:00:23:1b:41:46:a1:0c:
                    2d:c8:ec:90:8f:33:b6:62:46:f6:4e:65:02:65:e9:
                    93:62:e8:bf:b1:1d:33:21:b7:70:83:5c:5a:7c:a9:
                    7b:82:06:43:92:19:39:6a:73:ed:18:3c:49:c4:56:
                    a5:4d:8a:3a:fc:0e:59:42:ff:2e:6a:d6:da:26:00:
                    7f:1b:b5:4c:f0:6f:8e:f4:72:ee:71:a7:5a:77:6c:
                    d0:51:7a:50:7e:06:ca:dd:2f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Issuer Alternative Name:
                IP Address:2001:14:6CF:FAE7:BB79:BF78:7D64:C056
            X509v3 Subject Alternative Name:
                IP Address:2001:14:6CF:FAE7:BB79:BF78:7D64:C056
    Signature Algorithm: sha1WithRSAEncryption
        19:32:0b:72:a8:6c:f9:65:20:5b:1d:9a:e1:c7:39:97:c7:8a:
        4d:d1:01:f9:7d:0b:0d:6f:61:a2:e3:2c:62:30:28:f6:36:db:
        62:bc:7f:d1:9b:6d:cc:da:e3:9b:90:e7:53:9e:55:28:51:7e:
        39:de:23:24:f5:a9:97:7a:ba:ce:54:3e:cf:8b:68:04:f6:be:
        78:94:9f:d3:20:62:96:14:84:51:af:c7:ba:30:ae:b1:d6:7e:
        7f:32:42:9c:f6:f5:76:27:0a:28:58:8b:b5:85:e7:e9:5a:ff:
        aa:4c:57:55:95:09:33:ac:0b:8c:fd:05:4a:5e:60:e7:7f:d7:
        42:f0
```

Appendix C. Change log

Changes from version 00 to 01:

- Added cert types to use with hash and URL.
- Added how HITs should be represented in X.509.v3 certificates.
- Added full examples of SPKI and X.509.v3 certificates with HIP content
- Added and updated references
- Added reasons why to use certain messages to carry CERT parameter
- Added discussion about CRLs
- Removed the support for I1, because it may lead to DoS and middleboxes cannot be detected before its use

Authors' Addresses

Tobias Heer
Distributed Systems Group, RWTH Aachen University
Ahornstrasse 55
Aachen
Germany

Phone: +49 241 80 214 36
Email: heer@cs.rwth-aachem.de
URI: http://ds.cs.rwth-aachen.de/members/heer

Samu Varjonen
Helsinki Institute for Information Technology
Metsnneidonkuja 4
Helsinki
Finland

Fax: +35896949768
Email: samu.varjonen@hiit.fi
URI: http://www.hiit.fi

Full Copyright Statement

Intellectual Property