Workgroup: HIP
Internet-Draft:
draft-moskowitz-hip-hhit-registries-02
Published: 9 March 2020
Intended Status: Standards Track
Expires: 10 September 2020

Authors:	R. Moskowitz	S. Card	A. Wiethuechter
	HTT Consulting	AX Enterprize	AX Enterprize

Hierarchical HIT Registries

Abstract

This document describes using the registration protocol and registries to support hierarchical HITs (HHITs). New and existing HIP parameters are used to communicate Registry Policies and data about the HHIT device and the Registries. Further Registries are expected to provide RVS services for registered HHIT devices.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document expands on Hierarchical HITs [I-D.moskowitz-hip-hierarchical-hit], defining HIP registration protocol enhancements, the Registry services to support hierarchical HITs (HHITs), and given a HHIT, how to get additional information about the device.

Registries will tend to be organized regionally and by nature of their clients. For example, an RAA may be US centric and only have HDAs that are US-based.

Registries will need to work in a federation. Devices that are clients of one HDA/RAA will be needing information and connectivity to devices that are clients of other HDA/RAA. The policies for establishing such federations are outside the scope of this document.

Access to information at a Registry about a device may require authorization. The nature and process of such an authorization is outside the scope of this document.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Definitions

CSR (Certificate Signing Request):

Request to a Certificate Authority to create an X.509 certificate with the provided information.

HDA (Hierarchical HIT Domain Authority): The 14 bit field identifying the HIT Domain Authority under a RAA.

HID (Hierarchy ID): The 32 bit field providing the HIT Hierarchy ID.

RAA (Registered Assigning Authority): The 18 bit field identifying the Hierarchical HIT Assigning Authority.

RVS (Rendezvous Server): The HIP Rendezvous Server for enabling mobility, as defined in [RFC8004].

3. Problem Space

3.1. Desire for administrative control of HHITs

For HHITs to be effectively used, the HHIT Domain Authorities (HDAs) need to provide information on the HHIT devices. Minimally this would be the corresponding HI, information on the device owner (only to authorized requesters), and where in the network the device has last reported from.

The HHIT space creates a type of a business labeling for the HDAs. "These are my customers."

3.2. Desire for administrative control by RVS providers

An RVS [RFC8004] provider may only be willing to provide discovery (RVS) services to HIP devices it knows and trusts. A flat HIT space does not provide any intrinsic functionality to support this. A HHIT space can be mapped to the RVS provider. DNS can effectively be used to provide the HHIT to IP mapping without Distributed Hash Table (DHT) [RFC6537].

3.3. Defense against fraudulent HITs

How can a host protect against a fraudulent HIT? That is, a second pre-image attack on the HI hash that produces the HIT. A strong defense would require every HIT/HI registered and openly verifiable. With HHITs, the HDAs can provide the HI and proof of registration (e.g. X.509 certificate including HHIT).

This would best be done as either part of the R1 and I2 validation, or anytime a HHIT is presented.

4. HHIT Registry services to support hierarchical HITs

Hierarchical HIT registration SHOULD be performed using the HIP Registration Extension [RFC8003]. The client either uses an X.509 certificate [RFC8002], or use a PSK, as defined in Appendix A of HIP-DEX [I-D.ietf-hip-dex], to validate the registration.

The Registration should include additional client information. This information may be contained within the X.509 certificate (CERT parameter) and/or is carried in the CLIENT_INFO parameter, see Section 4.3.4. The Registrar can include its requirements in the R1 packet, and the client provide its information in the I2 packet. This parameter may be encrypted within the ENCRYPTED parameter. If the CLIENT_INFO contains Personal Identifying Information (PII), then it MUST be placed into the ENCRYPTED parameter.

The content and internal format of the CLIENT_INFO parameter is set by the HDA"s policy and is outside the scope of this document. Examples of client information can by phone number, IMEI, and ICCID.

4.1. Hierarchical HIT Registration using X.509 Certificates

This requires the HIP client to possess a client certificate trusted by the HDA/Registrar. Registration will either succeed or fail.

Certificate registration can be a "chicken and egg" problem: where did the device get its certificate? Thus this is more likely used in a re-registration situation with updated information.

4.2. Hierarchical HIT Registration using a PSK

This requires the HIP client and the HDA/Registrar to share a PSK. The PSK is carried in the ENCRYPTED_KEY parameter [I-D.ietf-hip-dex]. The PSK may already exist prior to starting the registration and just be used within the registration. A PSK out-of-band exchange may be triggered by performing the registration without any authentication.

If no client authentication is included in the I2 packet, the registration fails with "No Authentication provided". If the I2 packet included the proper HDA required client information, the HDA can use it to set up a side channel for an out-of-band delivery of a PSK. And example of this would be to send an SMS message with the PSK. Once the client possesses the PSK, it can rerun the registration at which point the HI and HIT duplicate checks are performed.

The I2 packet may contain a CERT parameter containing a CSR, and the R2 would return the X.509 certificate for later use.

4.3. HIP Parameters

The HIP parameters carry information that is necessary for establishing and maintaining a HIP association. For example, the device's public keys as well as the signaling for negotiating ciphers and payload handling are encapsulated in HIP parameters. Additional information, meaningful for end hosts or middleboxes, may also be included in HIP parameters. The specification of the HIP parameters and their mapping to HIP packets and packet types is flexible to allow HIP extensions to define new parameters and new protocol behavior.

4.3.1. CERT Parameter

The CERT parameter, [RFC8002], is a container for certain types of digital certificates.

A new CERT Type, CSR, is defined here. When CERT Type is CSR, CERT ID is Zero. There is only ONE CSR in a CERT Parameter.

CERT format	Type number	RFC
PKCS#10 - CSR	9	2986

4.3.2. Hierarchical HIT Registration Type

The Registration Type used in the REG_REQUEST is:

Number	Registration Type
2	HHIT Registration

4.3.3. Hierarchical HIT Registration Failure Type

The Registration may fail. In fact, with PSK, this may be the response to expect an SMS message with the PSK to use in a second registration request. Failure Types used in the REG_FAIL are:

Failure Type	Reason
[TBD-IANA]	Hierarchical HIT Already Registered
[TBD-IANA]	HI Already Registered
[TBD-IANA]	Previously Registered HI with different device information
[TBD-IANA]	No Authentication provided
[TBD-IANA]	Invalid Authentication
[TBD-IANA]	Invalid Authentication, new PSK sent via SMS

4.3.4. CLIENT_INFO

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             Type              |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   /                      Client Information                       /
   /                                                               /
   /                               +-------------------------------+
   /                               |            Padding            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

   Type           [TBD-IANA]
   Length         length in octets, excluding Type, Length, and
                  Padding
   Client         The information required by the HDA in the format
   Information    required by the HDA.
```

This parameter contains client information to include in the HIT registration. The specific content and format is set by the HDA.

4.4. Registration failure behavior

If the failure type is "Hierarchical HIT Already Registered", the client's HI is hashing to an existing HIT and must generate a new HI and hierarchical HIT and re-register. If the failure is "HI Already Registered", the client should assume it is registered. If the failure is "Previously Registered HI with different device information", either the client managed to generate a duplicate HI, possibly indicating a weak key generation algorithm, or the client was previously registered on a different device. Resolving this conflict will be left to the HDA's policy.

4.4.1. Example of a simple HDA policy

A simple HDA policy would be to require the device to generate a new HI and thus HHIT and try registration again. The HDA policy may also provide a URL for "Previous Registration Resolution". This contact is primarily to assist a device that was registered, but had some local failure resulting in a new registration attempt.

4.5. Example of a simple HDA policy

A simple HDA policy would be to require the device to generate a new HI and thus HHIT and try registration again. The HDA policy may also provide a URL for "Previous Registration Resolution". This contact is primarily to assist a device that was registered, but had some local failure resulting in a new registration attempt.

4.6. HHIT DNS Retrieval Service

A Registry SHOULD provide DNS retrieval services for the HIP RR [RFC8005] for HHITs as described in Hierarchical HITs [I-D.moskowitz-hip-hierarchical-hit].

This requires a Registry to act as a DNS zone Name Server to provide minimally the HI for the HHIT in the DNS query. Registry policy will determine if the response can be cached within DNS. If the Registry also provides the HHIT and/or the RVS for the HHIT, this may result in a different DNS caching policy by the Registry.

5. Using hierarchical HITs

All HIP clients with hierarchical HITs maintain an RVS connection with their HDA's RVS server(s). How the HDA scales this service up to a potential population in the millions is out of scope of this document. Lifetime management of these connections is also out of scope.

One approach an HDA can use to address the scaling challenge is to add an internal level of hierarchy to assign a set number of devices per RVS server.

Peering agreements between HDAs would allow for geographically close RVS to a device. This may reduce the latency for use of a device's current RVS. This is a subject of another document.

5.1. Contacting a HIP client

A service Initiator uses some service to discover the HIT of the service Responder. The Initiator uses the hierarchical information in the HIT to find the Responder's RVS. A trusted RVS discover method could use the DNS PTR to RVS as shown in Hierarchical HITs

[I-D.moskowitz-hip-hierarchical-hit]. An I1 is sent to that RVS which forwards it to the Responder.

The potential Responder uses the HIT in the I1 to query the Initiator's RVS about the Initiator. The nature of information, and method of communication are determined by the Initiator's HDA and the Responder's (and or HDA"s) relationship with it. Based on the Responder's local policy, this information will be used to determine if the contact is to be accepted. If accepted, the Responder may proceed sending an R1 to the Initiator. It may alternatively initiate some non-HIP process.

It should be noted that this R1 may contain a REG_INFO list for the Initiator to validate that the Responder does offer the desired service.

5.2. Defense against fraudulent HITs

Both the Initiator and Responder MAY validate a peer host as a defense against a second pre-image attack on the HHIT. This may occur via a CERT [RFC8002] in R1 or I2. It may be through a back end process associated with the R1 or I2 validation to look up the HHIT and retrieve the registered HI.

6. IANA Considerations

IANA will need to make the following changes to the "Host Identity Protocol (HIP) Parameters" registries:

CERT Type: This document defines the new CERT Type for the CERT parameter "PKCS#10 - CSR" (see Section 4.3.1).

Reg Type: This document defines the new Registration Type for the REG_REQUEST parameter "HIT Registration" (see Section 4.3.2).

Reg Fail: This document defines the new Failure Types for the REG_FAIL parameter (see Section 4.3.3).

CLIENT_INFO: This document defines the new CLIENT_INFO parameter (see Section 4.3.4). The parameter value will be assigned by IANA.

7. RAA Management Organization Considerations

Introducing the RAA management organization may be the largest hurdle for hierarchical HITs. Thus it would be best if this were adopted by an organization already in the business of allocating numbers within either the Internet or the Mobile, cellular, infrastructure.

One consideration would be to reserve the first N RAA values to map to the existing DNS TLDs. For example, these TLDs can be organized in an ascending order and numbered accordingly. Thus the 2 character TLDs will be a lower number than the 3 character TLDs. After that, it could be a first come, first numbered assignment process.

8. Security Considerations

There are potential risks with the hierarchical HIT, the Registry service, and the discovery of potential peer hosts using its hierarchical HIT.

A 64 bit hash space presents a real risk of second pre-image attacks. The HHIT Registry services effectively block attempts to "take over" a HHIT. It does not stop a rogue attempting to impersonate a known HHIT. This attack can be mitigated by the Responder using DNS to find the HI for the HHIT or the RVS for the HHIT that then provides the registered HI.

The two risks with hierarchical HITs are the use of an invalid HID and forced HIT collisions. The use of the "hhit.arpa." DNS zone is a strong protection against invalid HIDs. Querying an HDA's RVS for a HIT under the HDA protects against talking to unregistered clients. The Registry service has direct protection against forced or accidental HIT hash collisions.

By using the HIP Registration Extension, the Registry service is protected from direct attacks. This service does rely on either the integrity of a PKI service or an out-of-band PSK delivery process. Thus the risk to the Registry service is highly related to the trust in these authentication setup services. Further, the duplicate HI resolution process may require human interaction with related social engineering risks.

Finally the peer host discovery process relies on trusting the finding the proper HDA for the host and its forwarding the I1 to the proper Responder. A rogue RVS, impersonating the RVS for the HIT, could redirect the I1 to a client that has forced a collision with the HIT and the Initiator would be none the wiser. The only defense against this is if the Initiator has some other source for the Responder HI and validate the HI in the R1.

8.1. Privacy Concerns

Mobile-privacy-attack [I-D.moskowitz-mobile-privacy-attack] details how Eve can follow a communication between two mobile peers using the session Identifiers and deep knowledge about those Identifiers gained by hacking servers that log PII related to the Identifiers.

Hierarchical HITs not only does not mitigate this attack, it can actually aggravate it by supplying the HDA where the HHIT is registered.

A HIP Privacy Enhanced Base Exchange, to be defined in a separate draft, along with a Privacy Enhanced ESP tunnel, can be used to hide all the HIP and ESP Identifiers from Eve.

9. Acknowledgments

Sue Hares of Huawei contributed to the clarity in this document.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

[I-D.ietf-hip-dex] Moskowitz, R., Hummen, R., and M. Komu, "HIP Diet EXchange (DEX)", Work in Progress, Internet-Draft, draft-ietf-hip-dex-13, 14 February 2020, <https://tools.ietf.org/html/draft-ietf-hip-dex-13>.

[I-D.moskowitz-hip-hierarchical-hit]
Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", Work in Progress, Internet-Draft, draft-moskowitz-hip-hierarchical-hit-04, 3 March 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-hierarchical-hit-04>.

[I-D.moskowitz-mobile-privacy-attack]
Moskowitz, R., "An Attack on Privacy in Mobile Devices", Work in Progress, Internet-Draft, draft-moskowitz-mobile-privacy-attack-01, 13 November 2017, <https://tools.ietf.org/html/draft-moskowitz-mobile-privacy-attack-01>.

[RFC6537] Ahrenholz, J., "Host Identity Protocol Distributed Hash Table Interface", RFC 6537, DOI 10.17487/RFC6537, February 2012, <https://www.rfc-editor.org/info/rfc6537>.

[RFC8002] Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", RFC 8002, DOI 10.17487/RFC8002, October 2016, <https://www.rfc-editor.org/info/rfc8002>.

[RFC8003] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Registration Extension", RFC 8003, DOI 10.17487/RFC8003, October 2016, <https://www.rfc-editor.org/info/rfc8003>.

[RFC8004] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 8004, DOI 10.17487/RFC8004, October 2016, <https://www.rfc-editor.org/info/rfc8004>.

[RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 8005, DOI 10.17487/RFC8005, October 2016, <https://www.rfc-editor.org/info/rfc8005>.

Appendix A. Calculating Collision Probabilities

The accepted formula for calculating the probability of a collision is:

$$p = 1 - e^{-k^2/(2n)}$$

P	Collision Probability
n	Total possible population
k	Actual population

Authors' Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America

Email: rgm@labs.htt-consult.com

Stuart W. Card
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: stu.card@axenterprize.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: adam.wiethuechter@axenterprize.com