Workgroup: DRIP
Published: 27 April 2020
Intended Status: Standards Track
Expires: 29 October 2020
Authors: R. Moskowitz HTT Consulting
S. Card AX Enterprize
A. Wiethuechter AX Enterprize

UAS Remote ID

Abstract

This document describes using Hierarchical Host Identity Tags (HHITs) as a self-asserting and thereby trustable Identifier for use as the UAS Remote ID. HHITs include explicit hierarchy to provide registration discovery for 3rd-party ID assertion. Further, HHITs can also be used elsewhere in the UTM architecture to facilitate UAS communications.

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 https://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 29 October 2020.

Copyright Notice

Table of Contents

1. Introduction

This document describes the use of Hierarchical HITs (HHITs) [hierarchical-hit] as self-asserting and thereby a trustable Identifier for use as the UAS Remote ID. HHITs include explicit hierarchy to provide registration discovery for 3rd-party ID assertion.

The Drip Requirements [drip-requirements] describe a UAS ID as a "unique (ID-4), non-spoofable (ID-5), and identify a registry where the ID is listed (ID-2)"; all within a 20 character Identifier (ID-1).

HITs are statistically unique through the cryptograhic hash feature of second-preimage resistance. The addition of the Hierarchy and HHIT Registries [hhit-registries] provide complete, global HHIT uniqueness. This is in contrast to general IDs (e.g. a UUID or device serial number) as the subject in an X.509 certificate. All CAs within a PKI would have to check each other for duplicate (possibly fraudulent) IDs to approach this assurance of uniqueness.

Hierarchical HITs are valid, though non-routable, IPv6 addresses. As such, they fit in many ways within various IETF technologies.

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

CAA
: Civil Aeronautics Administration. An example is the Federal Aviation Administration (FAA) in the United States of America.

C2
: Command and Control. A set of organizational and technical attributes and processes that employs human, physical, and information resources to solve problems and accomplish missions. Mainly used in military contexts.

CS-RID
: Crowd Sourced Remote Identification. An optional DRIP WG service that gateways Broadcast RID to Network RID, and supports verification of RID positon/velocity claims with independent measurements (e.g. by multilateration), via a SDSP.

GCS
: Ground Control Station. The part of the UAS that the remote pilot uses to exercise C2 over the UA, whether by remotely exercising

UA flight controls to fly the UA, by setting GPS waypoints, or otherwise directing its flight.

HI
Host Identity. The public key portion of an asymmetric keypair from HIP.

HIP
Host Identity Protocol. The origin of HI, HIT, and HHIT, required for DRIP. Optional full use of HIP enables additional DRIP functionality.

HHIT
Hierarchical Host Identity Tag. A HIT with extra information not found in a standard HIT.

HIT
Host Identity Tag. A 128 bit handle on the HI. HITs are valid IPv6 addresses.

Observer
Referred to in other UAS documents as a "user", but there are also other classes of RID users, so we prefer "observer" to denote an individual who has observed an UA and wishes to know something about it, starting with its RID.

RID
Remote ID. A unique identifier found on all UA to be used in communication and in regulation of UA operation.

UA
Unmanned Aircraft. In this document UA's are typically though of as drones of commercial or military variety. This is a very strict definition which can be relaxed to include any and all aircraft that are unmanned.

UAS
Unmanned Aircraft System. Composed of Unmanned Aircraft and all required on-board subsystems, payload, control station, other required off-board subsystems, any required launch and recovery equipment, all required crew members, and C2 links between UA and the control station.

USS
UAS Service Supplier. Provide UTM services to support the UAS community, to connect Operators and other entities to enable information flow across the USS network, and to promote shared situational awareness among UTM participants. (From FAA UTM ConOps V1, May 2018).

UTM
: UAS Traffic Management. A "traffic management" ecosystem for uncontrolled operations that is separate from, but complementary to, the FAA's Air Traffic Management (ATM) system.

3. Hierarchical HITs as Remote ID

Hierarchical HITs are a refinement on the Host Identity Tag (HIT) of HIPv2 [RFC7401]. HHITs require a new ORCHID mechanism as described in [new-orchid]. HHITs for UAS ID also use the new EdDSA/SHAKE128 HIT suite defined in [new-hip-crypto] (requirements GEN-2). This hierarchy, cryptographically embedded within the HHIT, provides the information for finding the UA's HHIT registry (ID-3).

The current ASTM [F3411-19] supports three types of UAS IDs, namely the [CTA2063A] serial number, CAA registration ID and UTM-provided UUID session ID. For HHITs to be used effectively as UAS IDs, F3411-19 SHOULD add HHIT as the fourth UAS ID type.

3.1. Hierarchical HIT Registry

HHITs are registered to Hierarchical HIT Domain Authorities (HDAs) as described in [hhit-registries]. This registration process ensures UAS ID global uniqueness (ID-4). It also provides the mechanism to create UAS Public/Private data associated with the HHIT UAS ID (GEN-4 and GEN-5).

The 2 levels of hierarchy within the HHIT allows for CAAs to have their own Registered Assigning Authority (RAA) for their National Air Space (NAS). Within the RAA, the CAAs can delegate HDAs as needed. There may be other RAAs allowed to operate within a given NAS; this is a policy decision by the CAA.

3.2. Remote ID Authentication using HHITs

The EdDSA25519 Host Identity (HI) underlying the HHIT is used for the Message Wrapper, Sec 4.1 [drip-auth] (requirements GEN-2). It and the HDA's HI/HHIT are used for the Offline Claim, sec 4.3 [drip-auth] (requirements GEN-3). These messages also establish that the UA owns the HHIT and that no other UA can assert ownership of the HHIT (GEN-1).

The number of HDAs authorized to register UAs within an NAS determines the size of the HDA credential cache a device processing the Offline Authentication. This cache contains the HDA's HI/HHIT and HDA meta-data; it could be very small.

4. UAS ID HHIT in DNS

There are 2 approaches for storing and retrieving the HHIT from DNS. These are:

*As FQDNs in the .aero TLD.

*Reverse DNS lookups as IPv6 addresses per [RFC8005].

The HHIT can be used to construct an FQDN that points to the USS that has the Public/Private information for the UA (GEN-4 and GEN-5). For example the USS for the HHIT could be found via the following. Assume that the RAA is 100 and the HDA is 50. The PTR record is constructed as:

```
50.100.hhit.uas.areo   IN PTR      foo.uss.areo.
```

The individual HHITs are potentially too numerous to actually store in DNS. Rather the USS would provide the HHIT detail response.

The HHIT reverse lookup can be a standard IPv6 reverse look up, or it can leverage off the HHIT structure. Assume that the RAA is 10 and the HDA is 20 and the HHIT is:

```
2001:14:28:14:a3ad:1952:ad0:a69e
```

An HHIT reverse lookup would be to is:

```
2001:14:28:14:a3ad:1952:ad0:a69e.20.10.hhit.arpa.
```

5. Other UTM uses of HHITs

HHITs can be used extensively within the UTM architecture beyond for UA ID (and USS in UA ID registration and authentication). The GCS SHOULD have its own HHIT as an ID. It could use this if it is the source of Network Remote ID for securing the transport and for secure C2 transport [drip-secure-nrid-c2].

Observers SHOULD have HHITs to facilitate UAS information retrieval (e.g. for authorization to private UAS data). They could also use their HHIT for establishing a HIP connection with the UA Pilot for direct communications per authorization. Further, they can be used by FINDER observers, [crowd-sourced-rid].

6. DRIP Requirements addressed

This document provides solutions to GEN 1 - 6 and ID 1 - 5.

7. ASTM Considerations

ASTM will need to make the following changes to the "UA ID" in the Basic Message:

Type 4:
This document UA ID of Hierarchical HITs (see Section 3).

8. IANA Considerations

TBD

9. Security Considerations

The security considerations with Hierarchical HITs, most notably the short hash of the HI, are discussed in [hierarchical-hit]. The binding of the hierarchy to the hash of the HI is covered in [new-orchid].

Cryptographically Generated Addresses (CGAs) provide a unique assurance of uniqueness. This is two-fold. The address (in this case the UAS ID) is a hash of a public key and a Registry hierarchy naming. Collision resistance (more important that its implied second-preimage resistance) makes it statistically challenging to attacks. A registration process as in HHIT Registries [hhit-registries] provides a level of assured uniqueness unattainable without mirroring this approach.

The second aspect of assured uniqueness is the digital signing process of the HHIT by the HI private key and the further signing of the HI public key by the Registry's key. This completes the ownership process. The observer at this point does not know WHAT owns the HHIT, but is assured, other than the risk of theft of the HI private key, that this UAS ID is owned by something and is properly registered.

9.1. Hierarchical HIT Trust

The HHIT UAS RID in the ASTM Basic Message (the actual Remote ID message) does not provide any assertions of trust. The best that might be done is 4 bytes truncated from a HI signing of the HHIT (the UA ID field is 20 bytes and a HHIT is 16). It is in the ASTM Authentication Messages as defined in [drip-auth] that provide all of the actual ownership proofs. These claims include timestamps to defend against replay attacks. But in themselves, they do not prove which UA actually sent the message. They could have been sent by a

dog running down the street with a Broadcast Remote ID device strapped to its back.

Proof of UA transmission comes when the Authentication Message includes proofs for the Location/Vector Message and the observer can see the UA or that information is validated by ground multilateration [crowd-sourced-rid]. Only then does an observer gain full trust in the HHIT Remote ID.

HHIT Remote IDs obtained via the Network Remote ID path provides a different approach to trust. Here the UAS SHOULD be securely communicating to the USS (see [drip-secure-nrid-c2]), thus asserting HHIT RID trust.

10. Acknowledgments

TBD

11. 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>.

12. Informative References

[crowd-sourced-rid] Moskowitz, R., Card, S., and A. Wiethuechter, "Crowd Sourced Remote ID", Work in Progress, Internet-Draft, draft-moskowitz-drip-crowd-sourced-rid-03, 20 March 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-crowd-sourced-rid-03>.

[CTA2063A] ANSI, "Small Unmanned Aerial Systems Serial Numbers", September 2019.

[drip-auth] Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Authentication Formats", Work in Progress, Internet-Draft, draft-wiethuechter-drip-auth-00, 23 March 2020, <https://tools.ietf.org/html/draft-wiethuechter-drip-auth-00>.

[drip-requirements] Card, S., Wiethuechter, A., and R. Moskowitz, "Drone Remote Identification Protocol (DRIP) Requirements", Work in Progress, Internet-Draft, draft-

card-drip-reqs-02, 20 April 2020, <https://tools.ietf.org/html/draft-card-drip-reqs-02>.

[drip-secure-nrid-c2]
Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "Secure UAS Network RID and C2 Transport", Work in Progress, Internet-Draft, draft-moskowitz-drip-secure-nrid-c2-00, 6 April 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-secure-nrid-c2-00>.

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[hhit-registries]
Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HIT Registries", Work in Progress, Internet-Draft, draft-moskowitz-hip-hhit-registries-02, 9 March 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-hhit-registries-02>.

[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>.

[new-hip-crypto] Moskowitz, R., Card, S., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", Work in Progress, Internet-Draft, draft-moskowitz-hip-new-crypto-04, 23 January 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-new-crypto-04>.

[new-orchid] Moskowitz, R., Card, S., and A. Wiethuechter, "Using cSHAKE in ORCHIDs", Work in Progress, Internet-Draft, draft-moskowitz-orchid-cshake-00, 11 December 2019, <https://tools.ietf.org/html/draft-moskowitz-orchid-cshake-00>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[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>.

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