Workgroup: TMRID
Internet-Draft: draft-card-tmrid-uas-00
Published: 29 January 2020
Intended Status: Informational
Expires: 1 August 2020
Authors: S. Card A. Wiethuechter R. Moskowitz
AX Enterprize AX Enterprize HTT Consulting

UAS Remote ID

Abstract

This document is an Applicability Statement for various IETF Technical Specifications, complementing emerging external standards and regulations to meet needs for Unmanned Aircraft System (UAS) remote identification (RID). The objectives are: to facilitate use of existing Internet services to support UAS RID and to enable enhanced RID related services; and to enable verification that UAS RID information is trustworthy (to some extent, even in the absence of Internet connectivity at the receiving node).

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 1 August 2020.

Table of Contents

1. Introduction

2. Terms and Definitions

2.1. Requirements Terminology

2.2. Definitions

3. UAS RID Problem Space

3.1. Network RID

3.2. Broadcast RID

3.3. TM-RID Focus Problem Space

4. Alternatives for IETF work on Trustworthy IDs

4.1. Requirements of Trustworthy IDs

4.2. Currently selected IDs by ASTM

4.3. Options for Trustworthy IDs

5. IANA Considerations

6. Security Considerations

7. Acknowledgments

8. References

8.1. Normative References

8.2. Informative References

Authors' Addresses

1. Introduction

Emerging Civil Aviation Authority (CAA) regulations worldwide, exemplified by current United States (US) Federal Aviation Administration (FAA) rulemaking, will soon mandate, and many safety and other considerations dictate (even absent regulations), that Unmanned Aircraft Systems (UAS) be remotely identifiable. CAAs are

expected and FAA has stated its intent to require compliance with industry consensus standards.

ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041 (UAS Remote ID and Tracking), is a Proposed New Standard [WK65041]. It defines 2 means of UAS remote identification (RID): Network RID via the Internet; and Broadcast RID via a one-way data link direct from the Unmanned Aircraft (UA) to the observer's device. Network RID depends upon Internet connectivity between the observer and either the UA itself or any of various proxies. Broadcast RID should need Internet (or other Wide Area Network) connectivity only for UAS registry information lookup using the directly locally received UAS ID as a key.

The need for near-universal deployment of UAS RID is pressing. This implies the need to support use by observers of already ubiquitous mobile devices (smartphones and tablets). UA onboard RID devices are severely constrained in Size, Weight and Power (SWaP). Cost is a significant impediment to the necessary near-universal adoption of UAS send and observer receive RID capabilities. To accomodate the most severely constrained cases, all these conspire to motivate system design decisions, especially for the Broadcast RID data link, which complicate the protocol design problem: one-way links; extremely short packets; and Internet-disconnected operation of UA onboard devices. Internet-disconnected operation of observer devices has been deemed by ASTM F38.02 too infrequent to address, but for some users is important and presents further challenges.

Heavyweight security protocols are infeasible, yet trustworthiness of UAS RID information is essential. Even the most basic datum, the UAS ID string (typically number) itself, under [WK65041], can be merely an unsubstantiated claim.

Further, an ID is not an end in itself; it exists to enable lookups and provision of services complementing mere identification, e.g. dynamic establishment of secure communications between the observer and the UAS pilot. [WK65041] neither fully specifies nor appears to facilitate these functions, especially in the case where the observer lacks real time Internet access.

Finally, [WK65041] proposes the use of plaintext and mostly static UAS ID strings. Even if lookup from these to operator Personally Identifiable Information (PII) is successfully limited to strongly authenticated personnel, properly authorized per policy: static IDs enable trivial correlation of patterns of use, unacceptable in many applications, e.g. package delivery routes of competitors.

IETF can help by providing expertise as well as mature and evolving standards. Host Identity Protocol (HIPv2) [RFC7401] and its Domain Name System (DNS) extensions [RFC8005] can complement emerging external standards for UAS RID, to facilitate utilization of existing and provision of enhanced network services, and to enable verification that UAS RID information is trustworthy (to some extent, even in the absence of Internet connectivity at the receiving node).

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 Aviation Authority. 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.

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. In this document it is assumed that the HI is based on

a EdDSA25519 keypair. This is supported by new crypto defined in [I-D.moskowitz-hip-new-crypto].

HIT
: Host Identity Tag. A 128 bit handle on the HI. Defined in HIPv2 [RFC7401].

HHIT
: Hierarchical Host Identity Tag. A HIT with extra information not found in a standard HIT. Defined in [I-D.moskowitz-hip-hierarchical-hit].

UA
: Unmanned Aircraft. Typically a military or commercial "drone" but can include any and all aircraft that are unmanned.

UAS
: Unmanned Aircraft System. Composed of UA, 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 control station.

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

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).

RID
: Remote ID. System for identifying UA during flight by other parties.

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 ID.

UAS ID
Unique UAS identifier. Per [WK65041], maximum length of 20 bytes.

UAS ID Type
Identifier type index. Per [WK65041], 4 bits, values 0-3 already specified.

RID SP
UAS RID Service Provider. System component that compiles information from various sources (and methods) in its given service area.

RID DP
UAS RID Display Provider. System component that requests data from one or more RID SP and aggregates them to display to a user application on a device.

UAS RID Verification Service
System component designed to handle the authentication requirements of RID by offloading verification to a web hosted service.

3. UAS RID Problem Space

UA may be fixed wing Short Take-Off and Landing (STOL), rotary wing (e.g. helicopter) Vertical Take-Off and Landing (VTOL), or hybrid. They may be single engine or multi engine. The most common today are multicopters: rotary wing, multi engine. The explosion in UAS was enabled by hobbyist development, for multicopters, of advanced flight stability algorithms, enabling even inexperienced pilots tp take off, fly to a location of interest, hover, and return to the take-off location or land at a distance. UAS can be remotely piloted by a human (e.g. with a joystick) or programmed to proceed from Global Positioning System (GPS) waypoint to waypoint in a weak form of autonomy; stronger autonomy is coming. UA are "low observable": they typically have a small radar cross section; they make noise quite noticeable at short range but difficult to detect at distances they can quickly close (500 meters in under 17 seconds at 60 knots); they typically fly at low altitudes (for the small UAS to which RID applies, under 400 feet Above Ground Level in the US); they are highly maneuverable so can fly under trees and between buildings.

UA can carry payloads including sensors, cyber and kinetic weapons or can be used themselves as weapons by flying them into targets. They can be flown by clueless, careless or criminal operators. Thus the most basic function of UAS RID is "Identification Friend or Foe" to mitigate the significant threat they present. Numerous other

applications can be enabled or facilitated by RID: consider the importance of identifiers in many Internet protocols and services.

Network RID from the UA itself (rather than from a proxy) and Broadcast RID require one or more wireless data links from the UA, but such communications are challenging due to $SWaP constraints and low altitude flight amidst structures and foliage over terrain.

3.1. Network RID

Network RID has several variants. The UA may have persistent onboard Internet connectivity, in which case it can consistently source RID information directly over the Internet. The UA may have intermittent onboard Internet connectivity, in which case a proxy must source RID information whenever the UA itself is offline. The UA may not have Internet connectivity of its own, but have instead some other form of communications to a (typically ground) node that can relay RID information to the Internet; this would typically be the GCS (which to perform its function must know where the UA is) or USS (which in the UTM system is required to be kept informed by the UAS operator). The UA may have no means of sourcing RID information, in which case the GCS, USS or other proxy may source it. In the extreme case, this would be the pilot using a web browser to designate, to a USS or other UTM entity, a time-bounded airspace volume in which an operation will be conducted; this may impede disambiguation of ID if multiple UAS operate in the same or overlapping spatio-temporal volumes.

In most cases in the near term, if the RID information is fed to the Internet directly by the UA or remote pilot, the first hop data links will be cellular Long Term Evolution (LTE) or WiFi, but provided the data link can support at least IP and ideally TCP, its type is generally immaterial to the higher layer protocols. The ultimate source of Network RID information feeds a RID Service Provider (SP), which essentially proxies for that and other sources; the ultimate consumer of Network RID information obtains it from a RID Display Provider (DP). Each DP aggregates information from all SPs that have UA currently operating in the airspace for which that DP is cognizant.

Network RID is the more flexible and less constrained of the UAS RID means specified in [WK65041]. Any IETF work needed to support or leverage it is left for later efforts; it is not further addressed herein or in other initial tm-rid documents.

3.2. Broadcast RID

[WK65041] specifies 3 Broadcast RID data links: Bluetooth 4.X; Bluetooth 5.X Long Range; and Wifi with Neighbor Awareness

Networking (NAN). For compliance with this standard, an UA must broadcast (using advertisement mechanisms where no other option supports broadcast) on at least one of these; if broadcasting on Bluetooth 5.x, it is also required concurrently to do so on 4.x (referred to in [WK65041] as Bluetooth Legacy).

The selection of the Broadcast medium was driven by research into what is commonly available on 'ground' units (smartphones and tablets) and what was found as prevalent or 'affordable' in UA. Further, there must be an API for the UAS receiving application to have access to these messages. At this time, only Bluetooth 4.X support is readily available, thus the current focus is on working within the 26 byte limit of the Bluetooth 4.X "Broadcast Frame" that goes out on the beacon channels.

Finally, the 26 byte limit of the Bluetooth 4.1 "Broadcast Frame" strictly enforces the RID maximum length of 20 bytes.

3.3. TM-RID Focus Problem Space

TM-RID will focus on adding immediate usability, thus trust to, Broadcast RID. The one-way nature of Broadcast RID precludes any stateful security protocol. Under [WK65041], any UA can announce a RID and an observer would be seriously challenged to validate it or any other information about the UA looked up from it. Thus providing trust in the RID and related trust for all Broadcast messages is critical for the safe and secure operation of UAs.

Three levels of functionality will be considered:

1. verify that HHIT is duly registered with a known registry AND that any messages signed with its key came from it;

2. look up not only static UAS registry and dynamic UTM information but also Intenet direct contact information for services relating to the UA, its current mission, etc., including communications with the remote pilot (or proxy) and USS;

3. dynamically establish strongly mutually authenticated, E2E strongly encrypted communications with the UAS RID sender and entities looked up via (2) above.

4. Alternatives for IETF work on Trustworthy IDs

4.1. Requirements of Trustworthy IDs

Just a couple of requirements:

1. The ID MUST be 20 bytes or smaller.

2. It MUST be non-spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID).

3. In context (that is in a Remote ID Broadcast message), just the ID provides enough information on how at least the observer's USS (UAS Service Provider / Display Provider) can provide both public and private information on the UAS.

4.2. Currently selected IDs by ASTM

Now a little 'context' setting. ASTM has already defined a set of textual Remote IDs:

1 Serial Number [CTA2063A]

2 CAA Assigned ID

3 UTM Assigned ID [RFC4122]

The work here MUST surpass these in terms of Trustworthiness.

4.3. Options for Trustworthy IDs

The options found are:

1. X.509 certs where something like the cert sequenceNumber is the Remote ID.

2. Naming Things with Hashes, Section 8.2 of [RFC6920]

3. SSH keyID

4. HIT (Host Identity Tag) [RFC7401]

Option 1 is no better than what ASTM/FAA is considering for any of the current proposed types. Somehow, there will be a PKI and from that knowledge of the UAS is gained. This REQUIRES Internet Access (think disaster or other non-Internet situations) and a GLOBAL PKI (the UA flew from Canada to the US or UK to France post Brexit).

Option 2 meets requirements 1 and 2, but needs to be augmented so that the Hash provides context for 3. Is it supported for IPsec and/or QUIC for UAS/observer secure communications (NetworkID).

5. IANA Considerations

It is likely that an IPv6 prefix will be needed for the HHIT (or other identifier) space; this will be specified in other drafts.

6. Security Considerations

UAS RID is all about safety and security, so content pertaining to such is not limited to this section. UAS RID information must be divided into 2 classes: that which, to achieve the purpose, must be published openly in plaintext, for the benefit of any observer; and that which must be protected (e.g. PII of pilots) but made available to properly authorized parties (e.g. public safety personnel who urgently need to contact pilots in emergencies). Details of the protection mechanisms will be provided in other drafts. Classifying the information will be addressed primarily in external standards but also herein as needed.

7. Acknowledgments

The work of the FAA's UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) is the foundation of later ASTM and proposed IETF efforts. The work of ASTM F38.02 in balancing the interests of diverse stakeholders is essential to the necessary rapid and widespread deployment of UAS RID.

8. References

8.1. 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>.

[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>.

[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>.

8.2. Informative References

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

[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-03, 16 December 2019, <https://tools.ietf.org/html/draft-moskowitz-hip-hierarchical-hit-03>.

[I-D.moskowitz-hip-new-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>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <https://www.rfc-editor.org/info/rfc6920>.

[WK65041] ASTM, "Standard Specification for Remote ID and Tracking", September 2019.

Authors' Addresses

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

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

Email: rgm@labs.htt-consult.com