Workgroup: DRIP
Published: 6 April 2020
Intended Status: Standards Track
Expires: 8 October 2020

Authors: R. Moskowitz, HTT Consulting
S. Card, AX Enterprize
A. Wiethuechter, AX Enterprize
A. Gurtov, Linköping University

Secure UAS Network RID and C2 Transport

Abstract

This document provides the mechanisms for secure transport of UAS Network-RemoteID and Command-and-Control messaging. Both HIP and DTLS based methods are described.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document defines mechanisms to provide secure transport for the ASTM Network Remote ID [F3411-19] (N-RID) and Command and Control (C2) messaging.

A secure transport for C2 is critical for UAS Beyond visual line of sight (BVLOS) operations.

Two options for secure transport are provided: HIPv2 [RFC7401] and DTLS [DTLS-1.3-draft]. These options are generally defined and their applicability is compared and contrasted. It is up to N-RID and C2 to select which is preferred for their situation.

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

B-RID

Broadcast Remote ID. A method of sending RID messages as 1-way transmissions from the UA to any Observers within radio range.

BVLOS

Beyond visual line of sight. An adjectival phrase describing any information transfer that does not travel via LOS communications.

CAA

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

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.

LOS

Line Of Sight. An adjectival phrase describing any information transfer that travels in a nearly straight line (e.g. electromagnetic energy, whether in the visual light, RF or other frequency range) and is subject to blockage. A term to be avoided due to ambiguity, in this context, between RF-LOS and V-LOS.

N-RID

Network Remote ID. A method of sending RID messages via the Internet connection of the UAS directly to the UTM.

NETSP

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

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. Network RID endpoints

The FAA defines the Network Remote ID endpoints as a USS Network Service Provider (NETSP) and the UAS. Both of these are rather nebulous items and what they actually are will impact how communications flow between them.

The NETSP may be provided by the same entity serving as the UAS Service Provider (USS). This simplifies a number of aspects of the N-

RID communication flow. An Operator is expected to register a mission with the USS. If this is done via the GCS and the GCS is the source (directly of acting as a gateway), this could set up the secure connection for N-RID. The NETSP is likely to be stable in the network, that is its IP address will not change during a mission. This simplifies maintaining the N-RID communications.

The UAS component in N-RID may be either the UA, GCS, or the Operator's Internet connected device (e.g. smartphone or tablet). In all cases, mobility MUST be assumed. That is the IP address of this end of the N-RID communication will change during a mission. The N-RID mechanism MUST support this. the UAS Identity for the secure connection may vary based on the UAS endpoint.

3.1. N-RID from the UA

Some UA will be equipped with direct Internet access. These UA will also tend to have multiple radios for their Internet access. Thus multi-homing with "make before break" behavior is needed. This is on top of any IP address changes on any of the interfaces while in use.

3.2. N-RID from the GCS

Many UA will lack direct Internet access, but their GCS may be so connected. There are two sources for the GCS for the RID messages, both from the UA. These are UA B-RID messages, or content from C2 messages that the GCS converts to RID message format. In either case, the GCS may be mobile with changing IP addresses. The GCS may be in a fast moving ground device (automobile), so it can have as mobility demanding connection needs as the UA.

3.3. N-RID from the Operator

Many UAS will have no Internet connectivity, but the UA is sending B-RID messages and the Operator has an Internet Connected device that is receiving these B-RID messages. The Operator's device can act as the proxy for these messages, turning them into N-RID messages.

3.4. UAS Identity

The UA MAY use its RID private key if the RID is a HHIT [hierarchical-hit]. It may use some other Identity, based on the NETSP policy.

The GCS or Operator smart device may have a copy of the UA credentials and use them in the connection to the NETSP. In this case, they are indistinguishable from the UA as seen from the NETSP. Alternatively, they may use their own credentials with the NETSP which would need some internal mechanism to tie that to the UA.

4. Command and Control

Command and Control (C2) connection is between the UA and GCS. Often this over a direct link radio. Some times, particularly for BVLOS, it is via Internet connections. In either case C2 SHOULD be secure from eavesdroppers and tampering. For design and implementation consistency it is best to treat the direct link as a local link Internet connection and use constrained networking compression standards.

Both the UA and GCS need to be treated as fully mobile in the IP networking sense. Either one can have its IP address change and both could change at the same time (the double jump problem). It is preferable to use a peer-to-peer (P2P) secure technology like HIPv2 [RFC7401].

5. Secure Transports

The raw RID and C2 messages will be wrapped in UDP. These UDP packets will either be transported in ESP for the HPv2 approach or DTLS application messages for DTLS. In both cases header compression technologies SHOULD be used and negotiated based on policy.

For IPv6 over both WiFi and Bluetooth (or any other radio link), Robust Header Compression (ROHC) [RFC5795] and/or Generic Header Compression (6LoWAN-HGC) [RFC7400] can significantly reduce the per packet transmission cost of IPv6. For Bluetooth, there is also IPv6 over Bluetooth LE [RFC7668] for more guidance.

Local link (direct radio) C2 security is possible with the link's MAC layer security. Both WiFi and Bluetooth link security can provide appropriate security, but this would not provide trustworthy multi-homed security.

5.1. HIPv2 for Secure Transport

HIP has already been used for C2 mobility, managing the ongoing connectivity over WiFi at start of mission, switching to LTE once out of WiFi range, and returning to WiFi connectivity at the end of the mission. This functionality is especially important for BVLOS. HHITs are already defined for RID, and need only be added to the GCS via HHIT Registration [hhit-registries] for C2 HIP.

When the UA is the UAS endpoint for N-RID, and particularly when HIP is used for C2, HIP for N-RID simplifies protocol use on the UA. The NETSP endpoint may already support HIP if it is also the HHIT Registrar. If the UA lacks any IP ability and the RID HHIT registration was done via the GCS or Operator device, then they may also be set for using HIP for N-RID.

Further, double jump and multi-homing support is mandatory for C2 mobility. This is inherent in the HIP design. The HIP address update can be improved with [hip-fast-mobility].

5.2. DTLS for Secure Transport

DTLS is a good fit for N-RID for any of the possible UAS endpoints. There are challenges in using it for C2. To use DTLS for C2, the GCS will need to be the DTLS server. How does it 'push' commands to the UA? How does it reestablish DTLS security if state is lost? And finally, how is the double jump scenario handled?

All the above DTLS for C2 probably have solutions. None of them are inherent in the DTLS design.

5.3. Ciphers for Secure Transport

The cipher choice for either HIP or DTLS depends, in large measure, on the UAS endpoint. If the endpoint is computationally constrained, the cipher computations become important. If any of the links are constrained or expensive, then the over-the-wire cost needs to be minimized. AES-CCM and AES-GCM are the preferred, modern, AEAD ciphers.

For ESP with HIP [RFC7402], an additional 8 bytes can be trimmed by using the Implicit IV for ESP option [RFC8750].

NIST is working on selecting a new lightweight cipher that may be the best choice for use on a UA. The Keccak Keyak cipher in [new-crypto] is a good "Green Cipher". The Implicit IV, above, can be used as the Unique Value in the Keyak cipher, saving sending the UV in the ESP (or DTLS) datagram.

5.4. HIP and DTLS contrasted and compared

This document specifies the use of DTLS 1.3 for its 0-RTT mobility feature and improved (over 1.2) handshake. DTLS 1.3 is still an IETF draft, so there is little data available to properly contrast it with HIPv2. This section will be based on the current DTLS 1.2. The basic client-server model is unchanged.

The use of DTLS vs HIPv2 (both over UDP, HIP in IPsec ESP mode) has own pros and cons. DTLS is currently at version 1.2 and based on TLS 1.2. It is a more common protocol than HIP, with many different implementations available for various platforms and languages.

DTLS implements a client-server model, where the client initiates the communication. In HIP, two parties are equal and either can be an Initiator or Responder of the Base Exchange. HIP provides separation between key management (base exchange) and secure transport (for example IPsec ESP tunnel) while both parts are tightly coupled in DTLS.

DTLS 1.2 still has quite chatty connection establishment taking 3-5 RTTs and 15 packets. HIP connection establishment requires 4 packets (I1,R1,I2,R2) over 2 RTTs. This is beneficial for constrained environments of UAs. HIPv2 supports cryptoagility with possibility to negotiate cryptography mechanisms during the Base Exchange.

Both DTLS and HIP support mobility with a change of IP address. However, in DTLS only client mobility is well supported, while in HIP either party can be mobile. The double-jump problem (simultaneous mobility) is supported in HIP with a help of Rendezvous Server (RVS) [RFC8004]. HIP can implement secure mobility with IP source address validation in 2 RTTs, and in 1 RTT with fast mobility extension.

One study comparing DTLS and IPsec-ESP performance concluded that DTLS is recommended for memory-constrained applications while IPSec-ESP for battery power-constrained [Vignesh].

6. IANA Considerations

TBD

7. Security Considerations

Designing secure transports is challenging. Where possible, existing technologies SHOULD be used. Both ESP and DTLS have stood "the test of time" against many attack scenarios. Their use here for N-RID and C2 do not represent new uses, but rather variants on existing depoyments.

The same can be said for both key establishment, using HIPv2 and DTLS, and the actual cipher choice for per packet encryption and authentication. N-RID and C2 do not present new challenges, rather new opportunities to provide communications security using well researched technologies.

8. Acknowledgments

Stuart Card and Adam Wiethuechter provivded information on their use of HIP for C2 at the Syracuse NY UAS test corridor. This, in large measure, was the impetus to develop this document.

9. 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. Informative References

[DTLS-1.3-draft] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-dtls13-37, 9 March 2020, <https://tools.ietf.org/html/draft-ietf-tls-dtls13-37>.

[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>.

[hip-fast-mobility] Moskowitz, R., Card, S., and A. Wiethuechter, "Fast HIP Host Mobility", Work in Progress, Internet-Draft, draft-moskowitz-hip-fast-mobility-03, 3 April 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-fast-mobility-03>.

[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>.

[RFC5795] Sandlund, K., Pelletier, G., and L-E. Jonsson, "The RObust Header Compression (ROHC) Framework", RFC 5795, DOI 10.17487/RFC5795, March 2010, <https://www.rfc-editor.org/info/rfc5795>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks

(6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/info/rfc7400>.

[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>.

[RFC7402] Jokela, P., Moskowitz, R., and J. Melen, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)", RFC 7402, DOI 10.17487/RFC7402, April 2015, <https://www.rfc-editor.org/info/rfc7402>.

[RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <https://www.rfc-editor.org/info/rfc7668>.

[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>.

[RFC8750] Migault, D., Guggemos, T., and Y. Nir, "Implicit Initialization Vector (IV) for Counter-Based Ciphers in Encapsulating Security Payload (ESP)", RFC 8750, DOI 10.17487/RFC8750, March 2020, <https://www.rfc-editor.org/info/rfc8750>.

[Vignesh] Vignesh, K., "Performance analysis of end-to-end DTLS and IPsec-based communication in IoT environments", Thesis no. MSEE-2017: 42, 2017, <http://www.diva-portal.org/smash/get/diva2:1157047/FULLTEXT02>.

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

Andrei Gurtov
Linköping University
IDA
58183 Linköping
Sweden

Email: gurtov@acm.org