Workgroup: DRIP
Published: 1 April 2020
Intended Status: Standards Track
Expires: 3 October 2020
Authors: R. Moskowitz S. Card A. Wiethuechter
HTT Consulting AX Enterprize AX Enterprize

Operator Privacy for RemoteID Messages

Abstract

This document describes a method of providing privacy for Operator information specified in the ASTM UAS Remote ID and Tracking messages. This is achieved by encrypting, in place, those fields containing Operator sensitive data using a hybrid ECIES.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document defines a mechanism to provide privacy in the ASTM Remote ID and Tracking messages [F3411-19] by encrypting, in place, those fields that contain sensitive Operator information. An example of such, and the initial application of this mechanism is the Operator longitude and latitude location in the System Message.

It is assumed that the Operator registers a mission with a USS. During this mission registration, the Operator and USS exchange public keys to use in the hybrid ECIES. The USS key may be long lived, but the Operator key SHOULD be unique to a specific mission. This provides protection if the ECIES secret is exposed from prior missions.

The actual Tracking message field encryption MUST be an "encrypt in place" cipher. There is rarely any room in the tracking messages for a cipher IV or encryption MAC. There is rarely any data in the messages that can be used as an IV. A cipher that meets this requirement is SPECK [Need Reference]; which is an initial recommendation. There are risks with this cipher, only partially mitigated by the ephemeral nature of the sensitive Operator information in the Tracking messages and the short-lived nature of the ECIES secret. Other ciphers will be investigated.

Future applications of this mechanism may be provided. At that time, they will be added to 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

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

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

ECIES
Elliptic Curve Integrated Encryption Scheme. A hybrid encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-ciphertext attacks.

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.

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.

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

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. The Operator - USS Security Relationship

All CAAs have rules defining which UAS must be registered to operate in their National Airspace. This includes UAS and Operator registration in a USS. Further, operator's are expected to report flight missions to their USS. This mission reporting provides a mechanism for the USS and operator to establish a mission security context. Here it will be used to exchange public keys for use in ECIES.

The operator's public key SHOULD be unique for each mission. The USS public key may be unique for each operator and mission, but not required. For best post-compromise security (PCS), even the USS public key should be changed over some operational window.

The public key algorithm should be Curve25519 [RFC7748]. Correspondingly, the ECIES 128 bit shared secret should be generated using KMAC as specified in sec 5 of [new-crypto].

4. System Message Privacy

The System Message contains 8 bytes of Operator specific information: Longitude and Latitude of the Remote Pilot of the UA. The GCS can encrypt these as follows.

The 8 bytes of Operator information are encrypted, using the ECIES 128 bit shared secret with Speck64/128.

Bit 2 of the Flags byte is set to "1" to indicate the Operator information is encrypted.

The USS similarly decrypts these 8 bytes and provides the information to authorized entities.

4.1. Using AES in the System Message

If 2 bytes of the System Message can be set aside to contain a counter that is incremented each time the Operator information changes, AES-CTR can be used as follows.

The Operator includes a 64 bit UNIX timestamp for the mission time, along with its mission pubic key. The Operator also includes the UA MAC address (or multiple addresses if flying multiple UA).

The high order bits of an AES-CTR counter is constructed by the Operator and USS as: LTRUNC(HASH(MAC|UTCTime), 14).

AES-CTR would then be used to encrypt the Operator information.

5. IANA Considerations

TBD

6. Security Considerations

The use of Speck for the block cipher has risks. Speck has been extensively analyzed. The risk is mitigated as the key is used to protect a limited number of blocks. In a 4 hour mission with a System Message every 10 seconds, there are only 1,440 applications of the Speck cipher, provided that the operator reported to the UA a new location within those 10 second windows.

Further, an attacker has no known text after decrypting to determine a successful attack. There is no knowledge of where the operator is in relation to the UA. Only if changing location values "make sense" might an attacker assume to have revealed the operator's location.

6.1. Crypto Agility

The Remote ID System Message does not provide any space for a crypto suite indicator or any other method to manage crypto agility.

All crypto agility is left to the USS policy and the relation between the USS and operator. The selection of the ECIES public key algorithm, the shared secret key derivation function, and the actual symmetric cipher used for on the System Message are set by the USS which informs the operator what to do.

7. Acknowledgments

The recommendation to use Speck for the block cipher comes after discussions on the IRTF CFRG mailing list. Better known ciphers will not work for this situation without changes to the System Message content.

8. 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>.

9. Informative References

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

[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>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

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