Non-repudiation for Drone-Related Data

ICAO Drone Enable 2022

16 Nov 2022

Joseph Rios
Chief Technologist, Aviation Systems Division
NASA Ames Research Center

UTM data requirements

In order for UTM to support safe multiple UAS operations within and beyond visual line-of-sight, data related to weather, 3D structures, other aircraft, etc. must be made available. Describe the type of data needed to support safe operations, how that data is collected, maintained current, shared with operators, and whether standards for certain types of data are needed in terms of data quality (e.g. integrity, reliability, continuity and availability), security and resilience.

Drone Enable 2022 RFI

UTM Data Requirements

In order for UTM to support safe multiple UAS operations within and beyond visual line-of-sight, data related to weather, 3D structures, other aircraft, etc. must be made available. Describe the type of data needed to support safe operations, how that data is collected, maintained current, shared with operators, and whether standards for certain types of data are needed in terms of data quality (e.g. integrity, reliability, continuity and availability), security and resilience.

Drone Enable 2022 RFI

Non-repudiation

Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.

- National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5

Non-repudiation

Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.

- National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5

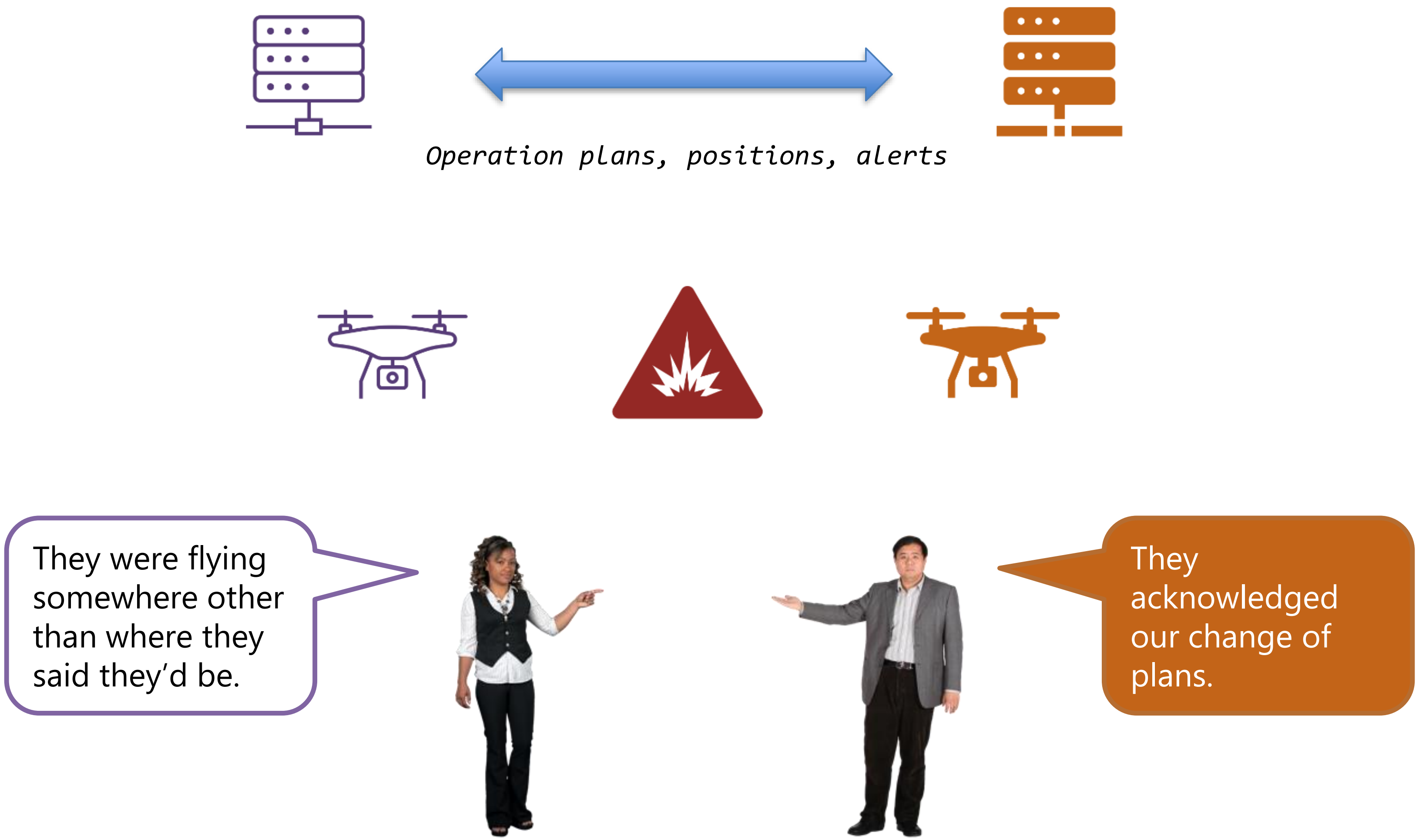
Why is non-repudiation important in UAS operations?

Increased Automation

Operator Collaboration

Building Trust

Operator-to-operator example



Operation plans, positions, alerts

They were flying somewhere other than where they said they'd be.

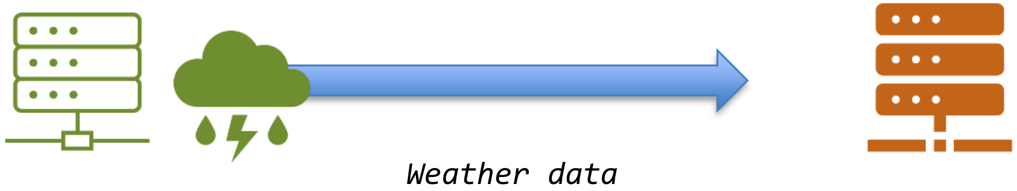
They acknowledged our change of plans.

Systems exchanging data per standards and airspace requirements.

Something bad happens between ops managed by different entities

Did they do what they said they would do?
Are they denying seeing data they actually saw?

Not just operation service suppliers…



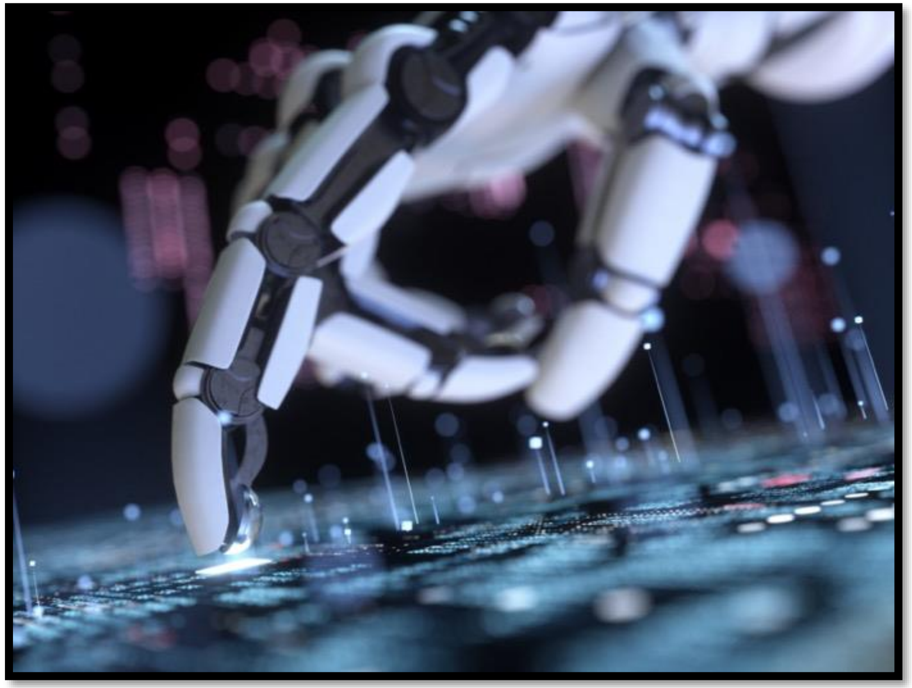
Operator receiving weather reports from a qualified provider

Operator ignores weather data or takes on excess risk, flying into bad conditions

You received a weather report and you didn't use it properly.
The weather report was wrong? I didn't get a report on time?

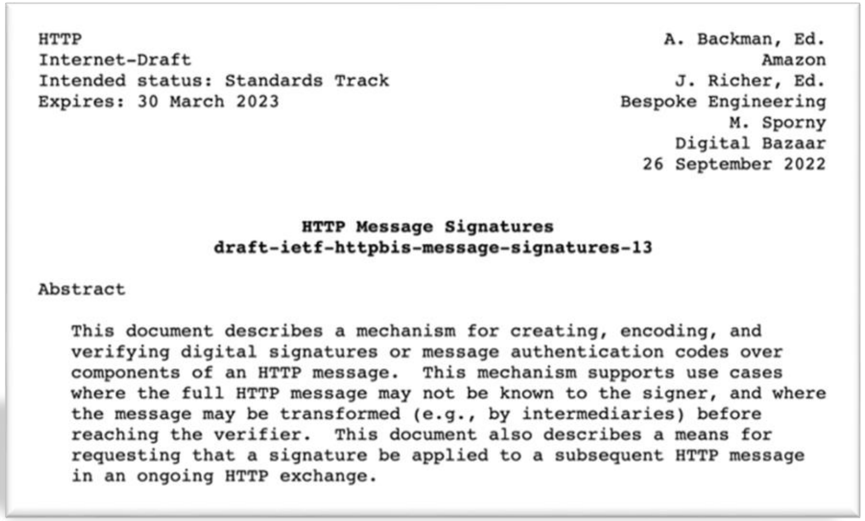
Operator claims a problem with weather service, insurance and weather provider disagree with operator

Message signing



Given appropriate infrastructure, it is possible to have each digital exchange signed, adding confidence that its content is unmodified and protecting against repudiation attacks against the system.

Proposed solution

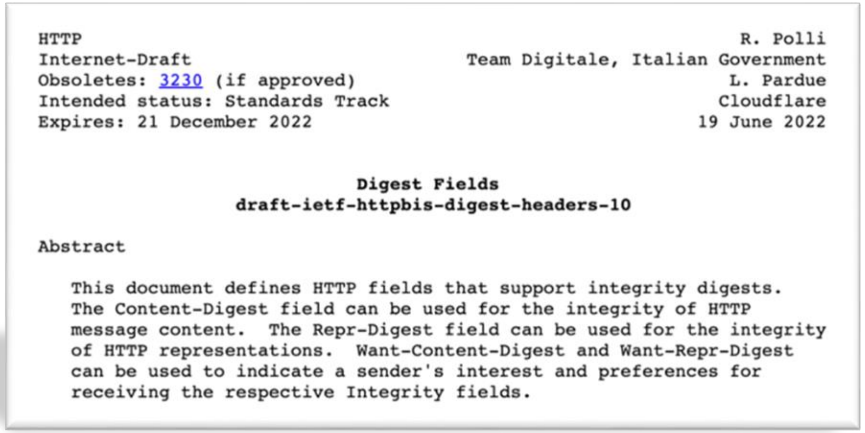


```
HTTP                                                  A. Backman, Ed.
Internet-Draft                                                 Amazon
Intended status: Standards Track                       J. Richer, Ed.
Expires: 30 March 2023                            Bespoke Engineering
                                                            M. Sporny
                                                       Digital Bazaar
                                                    26 September 2022


                        HTTP Message Signatures
              draft-ietf-httpbis-message-signatures-13

Abstract

   This document describes a mechanism for creating, encoding, and
   verifying digital signatures or message authentication codes over
   components of an HTTP message.  This mechanism supports use cases
   where the full HTTP message may not be known to the signer, and where
   the message may be transformed (e.g., by intermediaries) before
   reaching the verifier.  This document also describes a means for
   requesting that a signature be applied to a subsequent HTTP message
   in an ongoing HTTP exchange.
```



```
HTTP                                                         R. Polli
Internet-Draft                    Team Digitale, Italian Government
Obsoletes: 3230 (if approved)                               L. Pardue
Intended status: Standards Track                           Cloudflare
Expires: 21 December 2022                                19 June 2022


                             Digest Fields
                  draft-ietf-httpbis-digest-headers-10

Abstract

   This document defines HTTP fields that support integrity digests.
   The Content-Digest field can be used for the integrity of HTTP
   message content.  The Repr-Digest field can be used for the integrity
   of HTTP representations.  Want-Content-Digest and Want-Repr-Digest
   can be used to indicate a sender's interest and preferences for
   receiving the respective Integrity fields.
```

The Internet Engineering Task Force (IETF) has draft standards supporting non-repudiation of HTTP-based communications.

HTTP is the dominant approach to UAS Traffic Management (UTM) and xTM (extensible traffic management) system-to-system communications currently proposed, standardized, field-tested, and deployed around the world.

Careful consideration and implementation of these draft standards can close a gap that may otherwise derail faith and effectiveness of future UTM systems.

Currently being tested in the UTM Field Test in the USA. Regardless of those results, work would remain to fully vet and define requirements around message signing and non-repudiation.

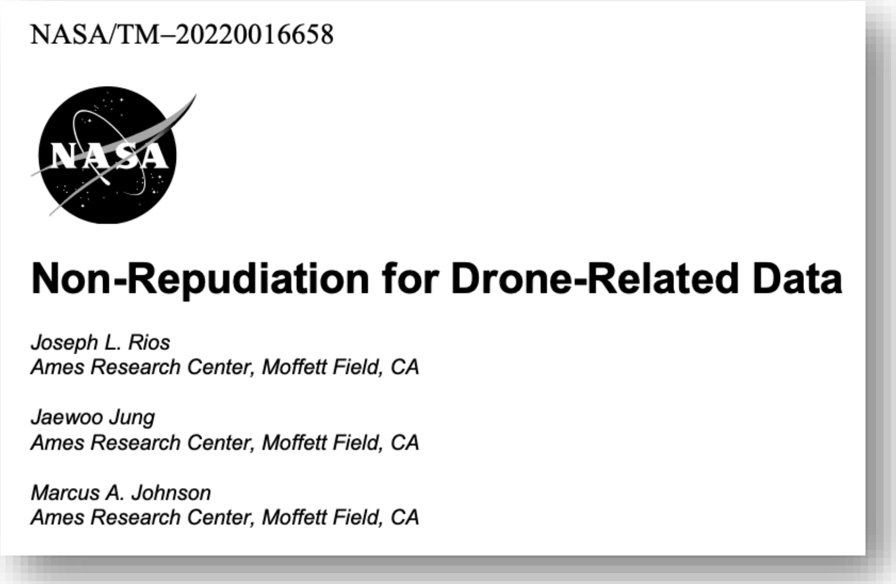
Concluding thoughts

Repudiation of digital exchanges can undermine confidence and effectiveness of xTM systems.

Previously there have not been standardized approaches to non-repudiation for HTTP exchanges, despite the recognition that it is an important part of message security.

Advances in standardization of non-repudiation coincide with the maturation of xTM systems and should be incorporated as early as possible in the operationalization process.

We have proposed an approach leveraging standards and understanding the current state-of-the-art in xTM systems.



NASA/TM–20220016658

Non-Repudiation for Drone-Related Data

Joseph L. Rios
Ames Research Center, Moffett Field, CA

Jaewoo Jung
Ames Research Center, Moffett Field, CA

Marcus A. Johnson
Ames Research Center, Moffett Field, CA

A detailed NASA Technical Memorandum on this topic is now available

Discussion and questions

Joseph Rios
NASA Ames Research Center

joseph.l.rios@nasa.gov