The DANCE of the UAs

draft-moskowitz-drip-secure-nrid-c2
July 28, 2022
Robert Moskowitz

Leveraging DANCE for Unmanned Aircraft Communications

Unmanned Aircraft Comm Basics

- Green field
  - Most communications today is LOS, often with no IP – this is changing
  - RF will be constrained capacity
- Two types
  - Command and Control (C2)
    - Between UA and Ground Control Station (GCS)
  - Network Remote ID
    - Telemetry to Unmanned Traffic Management (UTM)

Unmanned Aircraft Comm Basics

- Even autonomous operations need comm
  - C2 updates, both ways
    - But less traffic than non-autonomous operations
  - Telemetry always!
    - And if autonomous, it MUST be from the UA, not GCS
      - In non-autonomous, GCS gets telemetry as part of C2 anyway and may forward to UTM
    - Manned aircraft ADS-B not an option per regulators
  - Future of UTM re-routing directives direct to UA

Securing UA comm

- Two likely choices – ESP and DTLS
  - DTLS likely choice for most Network Remote ID
    - To fixed, known NRID Service Providers
    - But when UA on multiple interfaces, known problem with current DTLS code
      - Should be fixable
  - When GCS is mobile ESP via MOBIKE/HIP for C2
    - ESP in BEET mode naturally multi-homed
  - All in draft-moskowitz-secure-nrid-c2

UA Identities

- draft-ietf-drip-rid and -registries
    - DRIP Entity Tag (DET) is Hierarchical Host Identity Tag (HHIT), an update on rfc7401
        - DETs are ‘Session IDs” that may exist for the life of the UA or for a 30min “operation” (commonly called flight)
        - EdDSA25519 used for raw public key
        - Defined DNS FQDN for all DRIP enabled UA
            - If DET is not in DNS, DET was revocated
        - DETs stored in DNS with either/both HIP or TLSA RR
            - Raw Public Keys

UA Identities

- DETs in DNS trusted by
  - DNSSEC
    - Will this be possible for zones (run by HHIT Doman Authorities (HDA)) with hundreds of new DETs per hour be able to sign zone? TBD...
  - Registration Attestation in CERT RR via Private OID
    - See registries draft
    - Provides proof of registration and thus trust in DET

UA and DANCE when using DTLS

- We COULD send a rfc7250 raw public key of the HI, but then how to link that back the DET?
- Better to use DANCE with the known FQDN to retrieve everything from DNS.
  - The pieces just fit!
  - But server side may need special help on Attestations for trust

UA and DANCE when using DTLS

- If DRIP is widely adopted could mean millions of UAs in the coming years feeding telemetry into UTM.
  - Even if via GCS.
- Note C2 will tend to use pre-stored UA Identity for DTLS/ESP authentication
- More involved, but can work for other proposed solutions from other SDOs

QUESTIONS?