Secure Remote Drone ID: Implementation Updates

7th November 2023

IETF 118

Andrei Gurtov and TDDE21 students

LINKÖPING UNIVERSITY

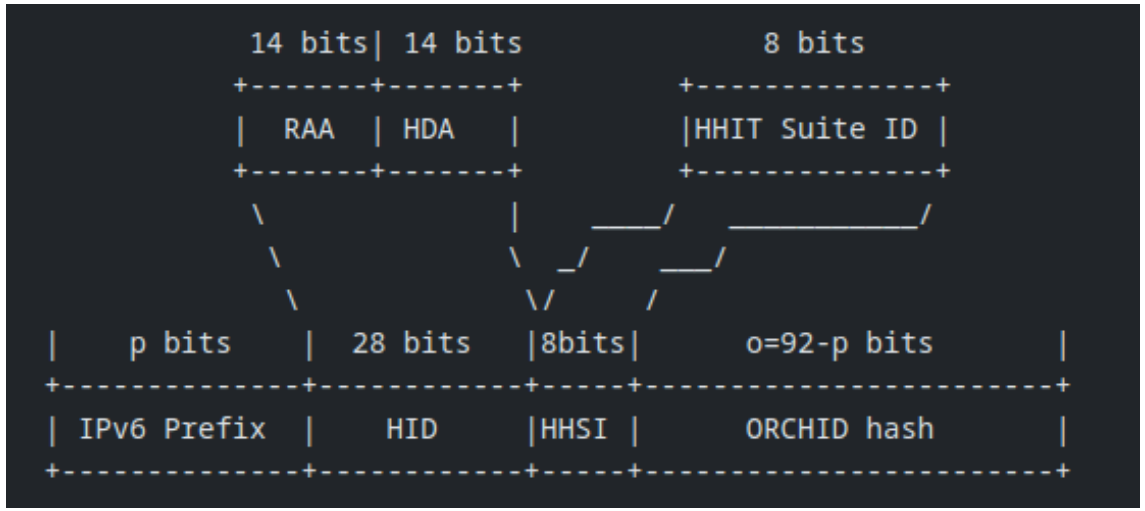
State of the art

- **DRIP (Drone Remote ID Protocol):** Enhancing drone accountability and safety through unique identification.
- **Hierarchical Host Identity Tag (HHIT):**
  - DET (DRIP Entity Tag): Uniquely identifies drones using a format based on IPv6, ensuring global uniqueness and ease of management.
- **Trustable identifiers:** Digital signatures from Assigning Authorities provide security and authenticity.
- **DNS as registry:** Decentralized method of managing drones identities, DNS servers in each country.

Changes from current HHIT to new according to RFC 9374

Old implementation (ORCHIDv2) for HIT only:

- 32 bits are used for the IPv6 prefix
- The OGA id / HHSI is 4 bits.
- The HI hash is the remaining 92 bits
- draft-moskowitz-hip-hierarchical-hit-05



In RFC 9374, the new ORCHID has the following format, and can be used for both HIT and HHIT:

- 28 bits for IPv6 prefix.
- The HID is 28 bits (for HHIT) or 0 bits (for HIT)
- The OGA id / HHSI is 8 bits (for HHIT) or 4 bits (for HIT)
- The HI hash is the remaining 64 bits (for HHIT) or 96 bits (for HIT) are used for the

Implementing the change in OpenHIP

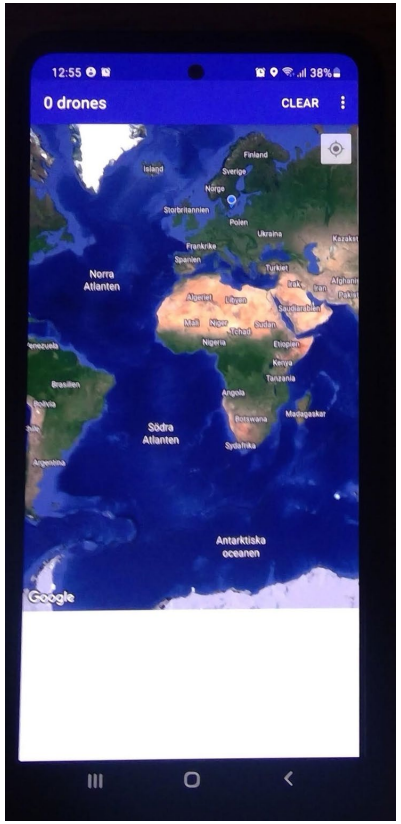
Current Status – RFC9374 and more

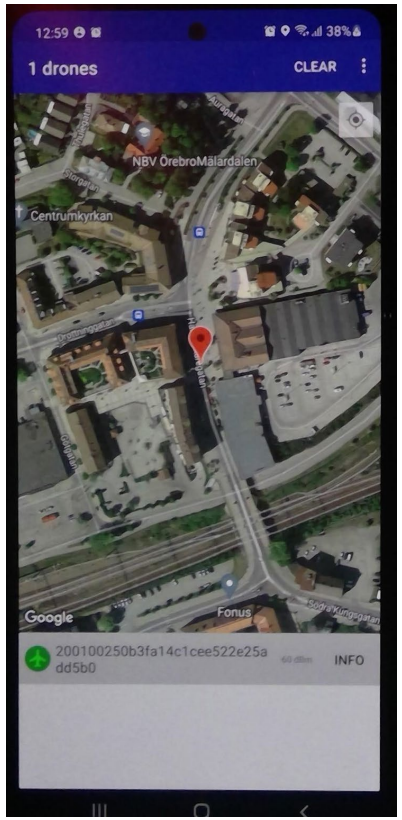
- Previous year implemented everything in draft-ietf-drip-rid-32
- Only cosmetic changes to the latest version (RFC9374)

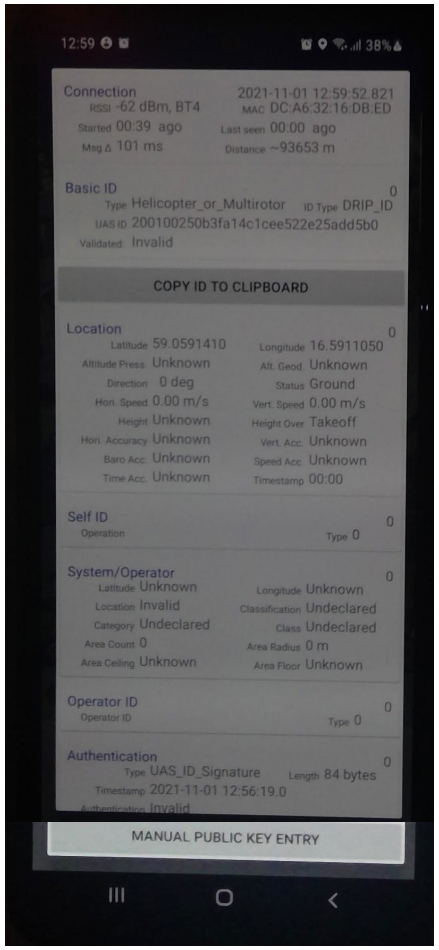
- Made latest way of generating HHITs compatible with previous code
- Converting an HHIT to a .xml file which is used by the transmitter (drone)
- Started making Android app compatible with transmitter code
  - Updated our web page https://www.ida.liu.se/~andgu38/drip/
  - https://gitlab.liu.se/hamro777/tdde21-drip-2022.git

Observer application

- OpendroneID as a base
- Custom backend DB/blockchain
  - Going to DNS
- Now published as Google Play App with OpenstreetMaps
  - A few tens of downloads
  - https://play.google.com/store/apps/details?id=org.securedroneid.android
  - iPhone next?







Main challenges so far - Authentication

- Last year implemented auth-17, upgrading to auth-31
- Follow the ASTM standard to prototype the different message types
- Understand the authentication draft and the interaction between the components
- Some message types are not fully specified
- Other messages include information that we don’t know how to access

Development strategy - DNS and certificates

- **Adapted IETF drafts and recommendations:** Utilized drafts and the IETF mailing list to figure out how integration between DNS and certificates works.
- **Local server setup for DNS using standard PC hardware:** Used Local DNS server in testing and proof of concept phase.
- **Version Control and Documentation:** Used Git to manage code changes and maintain documentation for the group and also for future projects.

Current status - DNS and certificates

- **Trying implementing registries-13**
- **Local DNS with BIND9:** Configured and operational, supporting drone-specific DNS queries.
- **Drone management:** Successful tests of registration and retrieval of Drone data on the DNS.
- **Certificate management:** Established process for generating the digital certificates needed.
- **Integration testing:** Tested compatibility and operation between DNS services and certificate management.
- DNSSEC?

Main challenges so far - DNS and certificates

- **Transitioning from TXT to unassigned DNS type (TYPE66):** Aligning with industry standards and best practices as per IETF mailing list recommendations.
- **Integration with existing systems:** Ensuring compatibility and seamless operation with backend and app from last year's project.
- **Testing and Quality Assurance:** So far the tests are limited in scope, so we are not sure if it is scalable.
- TODO: Integration with Android APP

OpenHIP Updates: C2 draft

- Changes since latest OpenHIP stable branch and latest
  - Porting of OpenSSL from v 1.1.1 to v 3.0.X
  - API for CORE functions (Emulator CORE v7.5 -> v9 porting)
  - Default libraries in Ubuntu
- What did work.
  - HIPv2 initialization
  - Communication path discovery.
- Issues
  - No IPsec communication after link establishment.
  - Debugging, documentation and automated test development
  - https://bitbucket.org/openhip/openhip/src/master/
- New HIPv2 implementation in Python
  - https://www.linuxjournal.com/users/dmitriy-kuptsov

Thanks!