Secure Remote Drone ID: Implementation and Experiment Updates

28\textsuperscript{th} March 2023
IETF 116

Andrei Gurtov
DRIP Experimental Testbed

- Observers receive Direct RID messages, and perform lookups on registry
- UAs and GCSs send location updates to registry
- Admin registers new accounts (drone/operators)
- UAs do not participate in the blockchain
Observer application

- OpendroneID as a base
- Google API with maps required separate developer key
  - Hard to provide .apk packages
- Now published as Google Play App with OpenstreetMaps
  - A few tens of downloads
  - iPhone next?
DRIP and Bluetooth 5

USB BT500

nRF52840 Dongle and Development Kit

Problem with Linux Drivers, also new external Bt5 dongle, now operational on RP4 after install of Ubuntu drivers. Drippy script updated for BT5. BT5 works in NUC.
A Master Thesis on DRIP Registries

• HL-DRIP: A Blockchain-based Remote Drone ID Protocol registry management - Evaluation of a Hyperledger Fabric-based solution to manage DRIP registries

• Juan Basaez, ~100 pages

• Completed, will be published soon at http://liu.diva-portal.org/
New Unit of Computing on DJI Matrics 300

- New Unit of Computing (NUC) Intel running DRIP remote ID over BT4 via API to a drone hardware (power, GPS)
- x86 architecture, Ubuntu Linux
- 5G modem
- Built-in BT4, BT5, WiFi
Formal Analysis of DRIP with Tamarin - Revising

<table>
<thead>
<tr>
<th>Lemma</th>
<th>Scope</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executable</td>
<td>Exists-trace</td>
<td>Verified</td>
</tr>
<tr>
<td>Session_key_secrecy</td>
<td>All-traces</td>
<td>Verified</td>
</tr>
<tr>
<td>Aliveness</td>
<td>HIP BEX Session Key</td>
<td>Verified</td>
</tr>
<tr>
<td>Weak agreement</td>
<td>HIP BEX Session Key</td>
<td>Verified</td>
</tr>
<tr>
<td>Non-injective agreement</td>
<td>HIP BEX Session Key</td>
<td>Verified</td>
</tr>
<tr>
<td>Injectable agreement</td>
<td>HIP BEX Session Key</td>
<td>Falsified</td>
</tr>
</tbody>
</table>

Diagram:
- (1) Generate HI keypair for himself.
- Generate certificate for himself (CO).
- Generate HI keypair for UA.
- Generate certificate for UA (CUA).
- (2) Send CO and CUA.
- (3) Receive CO and CUA.
- (4) Validate CO and CUA.
  Add UA to registry.
  Create proof of registration (CR).
  Create authentication component (AC).
- (5) Send UA’s HMIT etc. Send CR, Send AC.
- (6) Registry adds HMIT etc. to DNS.
- (7) Receive CR from registry. Receive AC from registry.
- (8) Send AC, Send UA’s keypair.
Wallenberg AI, Autonomous Systems and Software Program – New session in May

- Public Safety Arena (sea rescue)
- Demo at WASP-PS Arena (Thanks Tommy and AIICS group)
- Pick up BT4 signal at 160m using Galaxy 10 phone.
- Focus more on BT5 tests
- Integration to common visualization platform
Thanks! - Some backup slides (with links) attached
Hardware Kit for RP4

- Integrate with GPS and Battery Hat for on-the-drone mounting
- Antenna magnets disturbs drone compass -> remove!
DRIP on RP4 (ARM) and Phantom pro
DRIP Interops & IETF hackathon

- Interops at IETF’115 Hackathon (London, Nov 2022)
  - H_HIT format issues
  - Broadcast <-> app mutual compatibility
  - Adam Wiethuechter <adam.wiethuechter@axenterprize.com>
  - Their implementation is closed source
    - USA DoD demos at NY test site
- Our (LiU) is open source
OpenHIP Updates

Host Identity Protocol (HIP) is the inspiration for DRIP, also for C&C

https://bitbucket.org/openhip/openhip/src/master/

HHIT support, new crypto, HIPv2 branches

Added Docker container for easier cross-platform installation and testing
OpenSSL 3.0
Current Status

- OpenHIP used OpenSSL 1.0.x
- Added support for OpenSSL 1.1.0 in Fall 2020
- OpenSSL 3.0.0 was released in September 2021
- 1.1.1 support ends in September 2023

- Current OpenSSL implementation lacks forward compatibility
- High cohesion in the code that uses OpenSSL
- Large amount of deprecated methods
- Not all deprecated methods have one-to-one equivalents in 3.0.0
- Code compiles, but needs testing