DRIP Experiments Update

IETF 115, 10th November 2022

Andrei Gurtov and students
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
DRIP Interops & hackathon

- Some interop prior to IETF with Adam
  - H_HIT format issues
  - Broadcast <-> app mutual compatibility
- IETF Hackathon
  - Mutual testing of Android app and DRIP implementations
  - Some success, issues identified
DRIP and Bluetooth 5

nRF52840 Dongle and Development Kit

Problem with Linux Drivers, also new external Bt5 dongle, now operational on RP4 after install of Ubuntu drivers. Need to add options to our script. BT5 works in NUC.
Observer application

- OpendroneID as a base
- Google API with maps required separate developer key
  - Hard to provide .apk packages
- Now in the progress to publish as Google Play App with OpenstreetMaps
  - Much bureaucracy
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
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
Wallenberg AI, Autonomous Systems and Software Program

- 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.
- Also test OpenDroneID on NUC
  - Developed GPS patch
  - App backward compatible
Formal Analysis of DRIP with Tamarin

<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>Injective agreement</td>
<td>HIP BEX Session Key</td>
<td>Falsified</td>
</tr>
</tbody>
</table>

1. Generate H1 keypair for himself.
2. Generate certificate for himself (CO).
3. Generate H1 keypair for UA.
4. Generate certificate for UA (CUA).
5. Send UA’s H1IT etc. Send CR, Send AC.
6. Registry adds H1IT etc. to DNS.
8. Send AC. Send UA’s keypair.
OpenHIP Updates

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
- Support for OpenSSL 1.1.0 in Fall 2020
- OpenSSL 3.0.0 was released in September 2021
- 1.1.1 support ends in a year

- 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