In-orbit SW updates protection

Cyber-attacks are part of today's world. Not only in other industries but in space as well. Especially since 2022, the number of attacks skyrocketed and there is an unprecedented need for strong and reliable defense.

CORAC delivers end-to-end solutions that are acting as a safeguard against data interception, spoofing, and other malicious activities that have been targeting space asset data, as well as ground stations with high intensity.

How we help:

Software that is not digitally signed or is signed by an untrusted entity, can not be considered safe. Based on DevOps best practices, developers should be digitally signing commits, tags, entire containers, and whole SW packages distributed as SW updates. The same practice applies to the SW development process of space businesses.

CORAC solution offers both signing and verification capabilities on Earth as well as in space. Developers integrate CORAC KeyMaster crypto API to sign their SW updates and CORAC EPU crypto payload verifies SW updates after being transferred onboard a satellite.

How it works:

Users write code in their favorite IDE and push it to a CI/CD pipeline. One step of the pipeline automatically sent the hash value of pushed code to the CORAC KeyMaster API:

```
POST /signing/sign_hash
```

CORAC KeyMaster invokes a process for code signing and signs supplied hash with a code signing certificate linked to an identity of a certain user. Once signed, the code can be sent over an uplink to your satellite along with the corresponding public key. Onboard CORAC EPU payload then verifies the integrity of the received SW update and verifies the authenticity of the signature. As a result, the update can be installed because there is cryptographic proof that it was not modified by a malicious actor.