Uplink command protection

Radio communication between satellites and ground stations can be intercepted and various flaws in communication protocols can be exploited by cyber-criminals or state-sponsored adversarial groups in order to cause mission failure.

How we help:

CORAC solutions provide authenticity, integrity and protection against replay attacks focused on the uplink command channel. After an interception of uplink traffic, adversaries may resend intercepted commands and cause unpredictable damage to satellites (even though the command channel is encrypted).

It is also crucial to ensure the authenticity of commands received by your satellite and ensure that it accepts only commands created and sent by legitimate users and ground stations. The same degree of importance is given to the capability to prevent unauthorized processes or users to modify sent commands while in transit.

How it works:

CORAC KeyMaster allows the user to send the intended command "string" to its API endpoint for hash-based MAC (HMAC) signing.

```
POST /signing/sigh_HMAC
POST /signing/verify_HMAC
```

KeyMaster concatenates provided command string, shared secret, and command sequence number in order to feed CCSDS recommended SHA-256 (or SHA-3) hash function. As a result, KeyMaster produced a signed HMAC sent alongside the original command.

Once received by your satellite radio, onboard CORAC EPU payload uses a shared secret pre-burned to the EPU read-only memory and verification function that confirms that the command was not modified during the transfer, was created by a legitimate user, and was not reused by an adversary in order to conduct a replay attack.