Contribution ID: **20** Type: **lightning talk**

CubeCrypt - An Open-Source Implementation of Self-Signed ECC Certificates for CubeSat Telecommunication

Thursday, 9 December 2021 17:10 (5 minutes)

Despite the CubeSat industry becoming increasingly dominant within the space sector, it falls behind in one critical section: Cryptography. Current CubeSat security issues are often underestimated or neglected, despite the existing CCSDS standards for (all) satellite telecommunication. This is due to the fact that current CubeSat implementations simply do not require such strict security measurements. Nevertheless, due to the constant innovation within the space sector and the new threads these innovations could impose, cybersecurity in CubeSats will become crucial in the near foreseeable future. However, as security implementations on conventional satellites generally rely on hardware-based (FPGA / μ-controller) cryptography, the need for software-based cryptographic security solutions for the NewSpace industry have increased significantly.

This is where CubeCrypt comes into view: by creating a lightweight and open-source approach to satellite cryptography, it aims to become an software-based asymmetric cryptographic system suitable for CubeSat implementation. More specifically, the CubeCrypt system operates by utilizing ARMmbed's open-source mbedTLS library, by extending it to ensure no dynamic memory allocations are applied. In addition, CubeCrypt will be compiled for and implemented in bare-metal environments, ensuring its compatibility with space-grade on-board computers.

As an initial proof-of-concept, the CubeCrypt project will be used to establish the first foundation of cryptography: Authenticity. Rather than encrypting the data sent between a CubeSat and its ground-station, cryptographic certificates will be used to verify whether the CubeSat was truly sending the data, or whether someone else was trying to impersonate it. This will be done by creating self-signed X.509 ECC certificates and implementing them in the TRUST (Tamper-proof RandomnUmber generator from SaTellite) system, designed by the Department of Complex Systems Engineering (DISC) at ISAE-SUPAERO.

Primary author: ROELVINK, Yannick (ISAE-SUPAERO)

Co-authors: DETCHART, Jonathan (ISAE-SUAPERO); LACAN, Jérôme (ISAE-SUPAERO); GATEAU, Thibault (ISAE-SUAPERO)

Session Classification: Lightning Talks