Paper ID: 5042

EARTH OBSERVATION SYMPOSIUM (B1)
Earth Observation Data Management Systems (4)

Author: Mr. Carsten Tobehn
OHB System AG-Bremen, Germany, tobehn@ohb-system.de

Mr. Boris Penné
OHB System AG-Bremen, Germany, penne@ohb-system.de
Dr. Rainer Rathje
OHB System AG-Bremen, Germany, rathje@ohb-system.de
Dr. Andrew Weigl
OHB System AG-Bremen, Germany, weigl@ohb-system.de
Dr. Christian Gorecki
OHB System AG-Bremen, Germany, gorecki@ohb-system.de
Prof. Harald Michalik
IDA TU Braunschweig, Germany, michalik@hs-bremen.de

SECURITY CONCEPTS FOR EARTH OBSERVATION SATELLITES

Abstract

The high costs to develop, launch and maintain a satellite network makes protecting the assets imperative. Attacks may be passive such as eavesdropping on the payload data. More serious threat are active attacks that try to gain control of the satellite, which may lead to the total lost of the satellite asset. For security relevant applications also commercial system delivery today very high resolution data or other sensitive data, that can be misused. To counter these threats, new satellite and ground systems are using cryptographic technologies to provide a range of services: confidentiality, entity message authentication, and data integrity. Additionally, key management cryptographic services are required to support these services. The key points of current satellite control and operations are authentication of the access to the satellite TMTC link and encryption of security relevant TM/TC data. For payload data management the key points are multi-user ground station access and high data rates both requiring frequent updates and uploads of keys with the corresponding key management methods. For secure satellite management authentication key negotiation algorithms as HMAC-RIPEMD160, EC-DSA and EC-DH are used. Encryption of data uses algorithms as IDEA, AES, Triple-DES, or other. A channel coding and encryption unit for payload data handling provides download data rates up to Nx250 Mbps. This paper describes the key features relevant for security, as there are key management communication security methods and role based access control. The implementations of security units on-board the satellite, corresponding ground station units and EGSE as well as operational aspects of security are presented. The presented concepts are based on our experience and heritage of the security systems for all German MOD satellite projects (SATCOMBw2, SAR-Lupe multi-satellite system and German-French SAR-Lupe-Helios-II systems inter-operability) as well as for further international (KOMPSAT-II Payload data link system) and ESA activities (TMTC security and GMES concepts).