IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Space Communications and Navigation Global Technical Session (8-GTS.3)

Author: Dr. Kenneth Schmitz
OHB System AG, Germany, kenneth.schmitz@ohb.de

Mr. Helmar Hutschenreuter
OHB Digital, Germany, helmar.hutschenreuter@ohb.de

A WAY OUT: STANDARDIZED SPACE-TO-GROUND-TO-EVERYWHERE SECURITY

Abstract

A fundamental guideline for secure systems is that the strength of a solution should not depend on the secrecy of neither the implementation nor the architecture of the system. Instead, it should rely on universal best practices, correct implementations and established architectures. The current market of space-to-ground satellite link protection indicates a different philosophy on this matter. Specialized and mostly proprietary FPGA-based solutions are employed. Although extensively tested and, if necessary, certified by official entities, comprehensive reviews by the general public of experts is not possible. This makes it all the more likely that undiscovered security vulnerabilities may remain. It is often argued that it is impractical to connect to a satellite without special technical equipment. However, many information are standardized (CCSDS / ECSS) and readily available such that access in practice only depends on the effort the malicious party wants to invest. Whether on ground or in space, security is always a primary concern, when secret information are transmitted over a public channel. As a consequence, the largest system of systems – the internet – uses many technologies to protected secret information. To name only a few, OpenPGP, TLS or SSH are prominent examples of robust and de-facto secure implementations to ensure protection against adversary parties. Their implementations are mostly open source and the underlying algorithms have been widely reviewed and are still improving. However, security is not only based on the technical implementations themselves, but also on the correct interaction of different measures. Assume a network behind a firewall may still be misconfigured, such that adversary parties may extract data unnoticed. For this reason, any security solution must always consider all aspects. Generally, a risk analysis is carried out. Assets to be protected are identified and threats are analyzed. The need for protection is determined and adequate security measures are derived. National and international security standards exist to ensure a comparable level of security. The best known is probably the ISO27K series of standards. FPGA-based system designs are in some parts so special that state-of-the-art security measures cannot be applied unchanged. This leads to uncertainties in the implementation of security and to a level of security that cannot be clearly determined. Subsequently, we would like to propose a paradigm shift towards more standardized solutions even for the space-to-ground link protection. This solution is not FPGA, but software-based, lighter-weight, easier-to-deploy and addresses especially the needs of new space applications.