Paper ID: 1010
student

SPACE SYSTEMS SYMPOSIUM (D1)
Enabling Technologies for Space Systems (2)

Author: Mr. Daniel Fischer
University of Luxembourg, Luxembourg

Prof. Thomas Engel
University of Luxembourg, Luxembourg
Dr. Mario Merri
European Space Agency (ESA), Germany

IS INTERNET SECURITY GOOD ENOUGH FOR SPACE MISSIONS?

Abstract

The need for secure communications in open networks and especially the Internet is higher than ever before. Sophisticated, high quality commercial and open security solutions are available to satisfy this need. Until recently, security was not considered to be an issue for space missions. This has changed and many current and future missions have security requirements defined. Therefore, security technology in the internet is highly advanced when compared to the available solutions for civilian space missions. In our paper, we investigate and consider the spin-in of Internet security solutions to space mission architectures. Most security concepts for space missions are developed individually and from scratch while appropriate solutions may already be available for the Internet. Such a proprietary approach causes high development and maintenance costs and the added value in security is often negative when compared to open network solutions. The space environment has a number of restrictive properties such as isolation of the spacecraft, limited memory, bandwidth and computational resources that require simplification of adopted solutions. At the same time, the limited possibilities of an attacker and the restrictive behavior of the space environment can support these simplifications while maintaining the original level of security. In our paper we demonstrate that a careful adaptation of Internet based security solutions to space missions, which takes into account the above mentioned limitations, can greatly reduce complexity and produce highly efficient security service implementations. Such an adaptation requires a deep analysis with respect to cryptography, protocol design and overhead reduction. As a result of our considerations, we illustrate this concept on a concrete telecommand authentication solution, which has been chosen for ESAs future earth observation missions. While it is often discussed that proprietary solutions may provide a higher level of security through their secrecy, we argue that the adaptation of an open security specification provides a much higher level of security through many public reviews. Companies that have been selected to build a spacecraft with security requirements can much more easily re-use or adopt their existing expertise and security implementations, and therefore offer their services for a reduced price. To conclude, we propose mechanisms to adapt Internet proven security solutions in order to satisfy the security requirements of current and future space missions. The adaptation process is cheap and avoids the need for proprietary developments that cause unnecessary costs.