52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Interactive Presentations - 52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (IP)

Author: Dr. Jeremy Straub
North Dakota State University, United States

SECURING THE FINAL FRONTIER: A REVIEW OF SECURITY CHALLENGES AND A DISCUSSION OF SOME PROSPECTIVE SOLUTIONS AND WHAT CAN'T BE SOLVED

Abstract

With spacecraft lifetimes spanning decades, the security landscape was dramatically different when many current spacecraft were launched, than it is today. Mission planners must also assume that current security technologies will be obsolete within their mission's lifespan (perhaps dozens of times over for multi-decade missions). In addition to the obsolescence of software components, which can be updated, hardware obsolescence's security implications must also be considered. Obsoleted hardware can be problematic, as it may not support newer hardware security features (necessitating that they be performed in software). Hardware may also not have the processing capabilities required to support newer security technologies' processing requirements (within responsive timeframes).

This paper begins with a discussion of existing space mission security technologies (both historic and modern day) and their deficiencies. Gap analysis is performed for an example historic mission and an example modern-day mission. Based on this gap analysis several concerns for currently operating missions are raised. The paper then continues to consider a number of current security approaches to space missions and anticipates several potential future technical developments. The efficacy of these current security technologies is assessed under several scenarios of future technical development, some of which may aid the technology (such as increased processing capabilities at ground stations) and others which may impair the operations of the technology.

Focus then turns to approaches to make spacecraft security more future-proof. Approaches such as manually generated one time use codes, incorporating processing capabilities for security purposes beyond initial needs, being able to task security tasks to primary and payload processing hardware and incorporating a capability for secure updates to security systems are discussed and evaluated. The use of replaceable security hardware modules (which contain all of the hardware and software required for security purposes and operate across a common and well-defined interface to the rest of the spacecraft) is also presented. These modules could potentially be replaced, for Earth-orbiting missions, as part of a mid-mission refit, potentially using a small-size unmanned service craft.

After considering all of these prospective approaches, the paper then continues with a discussion of what cannot be readily solved and the implications of these limitations. This discussion considers these non-solvable problems from the perspective of an Earth-orbiting spacecraft as well as a more distant (and non-serviceable) one. The paper concludes with a discussion of the implications of these remaining gaps on space mission security, both now and in the future.