Paper ID: 62927
oral

IAF SPACE SYSTEMS SYMPOSIUM (D1)
Lessons Learned in Space Systems: Achievements, Challenges, Best Practices, Standards. (5)

Author: Mr. Edwin Betar
Boeing, Australia, ebetar@gmail.com

Mr. Mark Cross
Boeing, Australia, mark.s.cross2@boeing.com
Mr. Robert Hartley
Australia, robert.e.hartley@boeing.com
Mr. Tim Kent
Boeing, Australia, timothy.j.kent@boeing.com
Mr. Stephen Glass
Boeing, Australia, Stephen.M.Glass@boeing.com
Ms. Natalie Harris
Boeing, Australia, Natalie.Harris@boeing.com

SECURING YOUR PAYLOADS AGAINST THE SPACE CYBER KILL CHAIN:

Abstract

Earth orbiting satellite activities are evolving into increasingly mainstream, and could one day could be standardized to the point of being as nearly commoditized as internet web servers. In an age where satellite technology is becoming increasingly open source, this standardization allows more thorough and repeatable security efforts compared to bespoke systems of the past.

Ensuring that the space based ecosystem has cyber security built in means that that your space based fleet is secure from its orbiting neighbors, and rogue ground stations below.

The Boeing Defense Australia (BDA) cyber security team includes former industry and government hackers, security testers and software developers share their experiences developing methodologies, tools and procedures for testing Earth orbiting payloads.

They discuss what makes security testing satellites different from terrestrial communications and industrial control systems, and their unique experiences built up while developing and security testing delay tolerant networking systems, authentication and authorization systems and encryption for communications in transit and data at rest.

Sharing testing openly will help ensure that as utility satellites become increasingly standardized and open sourced, security will not be a unique competitive advantage, but something the community of satellite customers and operators can rely on, leaving them to compete on features and price.

Boeing Defense Australia's new methodologies include updated penetration testing procedures, robust testing of ground station and standard protocol implementations as well as software upload and update procedures. They help ensure that robust and redundant fail safe operational systems are secure and reliable in the extreme environment of space.