Paper ID: 49838
oral

52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Mr. Richard Linger
United States

BEHAVIOR COMPUTATION TO VALIDATE AEROSPACE SOFTWARE CYBER SECURITY: A KNOWLEDGE MANAGEMENT PROCESS

Abstract

Aerospace systems constitute a critical national infrastructure for defense, communications, navigation, and transportation. This infrastructure is subject to persistent attack and compromise by skilled adversaries seeking to disable capabilities essential to modern society. Because these systems are software enabled, attacks focus on software as a conduit to exfiltrate data, disrupt operations, or even repurpose functionality for hostile objectives.

It has never been more important to ensure that aerospace software is free of malicious content in both development and operation. In this connection, it is well understood that software with unknown behavior has unknown security. Software can exhibit unknown behavior inadvertently programmed by developers or inserted by adversaries during development or operation. Complex supply chains compound the problem with software whose full functionality and provenance may not be known.

Recent advances in the science and technology of software behavior computation provide a powerful means to validate the functionality and security of aerospace software. Behavior computation does not rely on traditional, approximate methods such as scanning or execution of code. Instead it applies mathematical foundations to derive the as-built behavior of software. Behavior computation operates on deep functional semantics and is guided by key theorems dealing with the structure and functionality of software. At the level of computed behavior, malware hidden in code by adversaries becomes visible and its functionality and objectives become apparent. Behavior computation essentially automates reverse engineering of software. This technology is currently being applied in federal and commercial organizations to help ensure operational security.

In a broader context, aerospace software embodies a massive amount of valuable design knowledge locked into syntactic forms that mask and obscure it. Behavior computation liberates this knowledge by revealing how software works. This knowledge can be applied to validation of security and functionality and enable confident software reuse and recombination. In short, software paired with its computed behavior is more valuable and useful than the software alone. Behavior computation produces new knowledge artifacts, previously unavailable, that can be captured, used, secured, and shared in a knowledge management framework for aerospace software development and operations.

This paper describes software behavior computation technology and illustrates its application to derive the behavior of an example program that contains malicious operations hidden within legitimate functionality. The paper also discusses knowledge management implications of the technology in terms of support for aerospace workforce productivity, software quality and security, and operational safety and reliability.