Paper ID: 28741
oral

48th SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Dr. Nitzan Barkay
Israel Aerospace Industries. Ltd, Israel

Ms. Esti Peshin
Israel Aerospace Industries. Ltd, Israel
Mr. Amir Paz
Israel Aircraft Industries Ltd., Israel
Mr. Amir Shlomo
Israel Aerospace Industries. Ltd, Israel
Dr. Yiftah Lipkin
Israel Aerospace Industries. Ltd, Israel

CYBER HARDENING & CYBER EARLY WARNING AS BUILDING BLOCKS IN SATELLITE CYBER WORTHINESS

Abstract

We are witnessing a proliferation of studies, researches information related to vulnerabilities, weaknesses and risks in operational systems (including but not limited to satellites, satellite communication systems, aviation systems, military systems and more). This information, which in some cases, is easily accessible via the Internet, includes in some cases "how to" information, which can be utilized by malicious attackers, as building blocks for instigating targeted attacks against operation systems. As such, operational systems can no longer rely on security by obscurity, and must ensure active measure to ensure their continuous cyber worthiness. This paper will discuss two complementary approaches for enhancing cyber situation awareness of satellite systems, and the probability of detecting sophisticated attacks involving subtle effects, without the penalty of too much false alarms. The first approach consists of a layered "cyber hardening" framework, taking into account the IT communication components of satellite systems and ground stations, as well as the unique properties of such systems. The second approach focuses on decision making - essentially what types of anomalies should be reported and subsequently handled – in order to provide efficient early warning, when preemptive action can still be employed. In the context of both approaches, we will discuss the commonality of cyber warfare related to operational systems to the legacy Electronic Warfare (EW) domain and look for more insight and hints to possible adoption of methods. The two combined approaches enable improving the probability of detection of a cyber attack, while maintaining a more resilient system on one hand, and reporting more reliable alerts to reduce false alarms, on the other hand. We will focus on the multi hypothesis tracking (MHT) methodology. MHT processes associate dynamic data from various sources, when the data is partial, ambiguous or uncertain, to generate alerts of cyber tracks. Associating distinct events to a possible single incident track, enables verification of consistency, may direct backwards investigation including clues for actor trend behavior and forward estimation of possible future impact. Utilizing MHT allows reporting high-score solutions, while maintaining and managing a multiple number of hypotheses and deferring decision, in anticipation that subsequent data provides better resolution. We will elaborate on the MHT algorithm stages and discuss in the adaptations to satellite systems. Moreover, reported cyber tracks would already include the necessary data for incident response: the associated events, possible actor attribution and estimated future impact.