Executive Summary

Commercial Space System Security Guidelines

Edited by Harrison Caudill & Chris Wake, Orbital Security Alliance

rev-1.0.1 – February 1, 2020

There is a strong need for improved security in commercial smallsat systems. In the Orbital Security Alliance's (OSA's) previous paper, *Big Risks in Small Satellites*, it was shown that use of secure infrastructure can not only help to defend the market from advanced threats, but also simultaneously decrease startup, development, and compliance costs. That model of leveraging secure infrastructure provides the necessary economic and operational breathing room for effective security measures to be deployed. This paper provides some guidelines for those security measures. A combination of immediately actionable security guidelines are presented, in addition to some techniques which are not yet widely available but are expected to be production-ready in the near future. These guidelines are intended to transition the conversation within industry and within the security community away from the general to the specific, and then to provide guidance to practitioners regarding the extent to which these security measures should be applied without being overly-prescriptive.

Operational Integrity of TT&C

Karl Mattson *LA Cyber Lab*

The Telemetry, Tracking, & Control (TT&C) communications link on a satellite is of critical importance to mission success and asset security. Without that link, the spacecraft state cannot even be determined to say nothing of any exercise of control over it. TT&C system integrity must be assured.

We find a useful and relevant comparison of the TT&C systems to the global banking system's Society for Worldwide Interbank Financial Telecommunication (SWIFT) network. Global financial institutions perform over 24 million transactions amongst 10,000 member organizations across the SWIFT network every day. The daily value of money transacted over the SWIFT network is over $5 trillion per day ($1.25 quadrillion dollars annually), making it vital to economic health around the world. While SWIFT member institutions have been victimized by cyber fraud, such as the Bank of Bangladesh attack in 2016, the overall integrity of the SWIFT network itself is remarkably successful by any measure. This track record of success may be brought to the space industry to protect the crucial TT&C link.

Guidelines for Physical Layer Security

Mark Lombardi, James Low, & Phil Trainor *Keysight Technologies*

The physical layer of a wireless communications link is extremely difficult to do well, even at the best of times. Outside of a lab, a large number of issues may arise making for less-than-optimal conditions. Since even basic reliability is a critical component of link availability (i.e. the ability to communicate with a satellite), basic practices such as trust-but-verify for vendor-supplied and internally-produced components alike are

info@orbitalsecurity.space

encouraged. Additionally, many of the methods utilized to defend a wireless link against unintentional jamming and disruption are effective against a deliberate attack. Many of the security and reliability lessons learned at great expense in the cellular industry are transferrable to the space industry.

Intelligence: Local Monitoring

Arun Viswanathan *Jet Propulsion Laboratory*

It is crucial to ensure that local monitoring is occurring and being fed into the overall threat intelligence picture. The Jet Propulsion Laboratory (JPL) plans to publish a set of lessons learned and best practices on this topic in the future. The OSA would like to refer readers to the impending publication by Dr. Arun Viswanathan and members of the Cyber Defense Engineering and Research Team at JPL.

Intelligence: The IoT Crisis

Garry Drummond *802Secure*

Connected devices are ubiquitous, existing everywhere that people spend time, from home to work to the supermarket. Unfortunately, the proliferation of IoT connected devices is proving to be a double-edged sword. For all of the benefits that IoT brings to the Enterprise, Government and Public Services, the sheer volume of intelligent IoT endpoints is proving to be a cybersecurity nightmare: networks that were once air-gapped are now connected to the internet, creating an ever-expanding attack surface. Each IoT device is yet another entry point for attack.

IoT broadly includes everything that traditionally was not connected to the public internet but now can communicate with the internet with little management or oversight. A forecast from IDC estimates that there could be more than 40 billion IoT devices connected by 2025.

Wireless is the new network and new attack surface, with an estimated 80% of IoT devices now connected wirelessly. In addition, IoT introduces a plethora of new operating systems, new protocols, and new frequencies that traditional IT and Information Security teams are unfamiliar with, which has created new security blind-spots.

Intelligence: Threat Intelligence Platforms

Chris Adams *ThreatConnect Inc.*

Despite massive investments in standard security devices (firewalls, endpoint protection, etc.), organizations continue to be hacked. That doesn't mean these devices no longer serve a purpose, but it's fair to say security architectures must evolve as adversarial tactics and techniques evolve. The first step in this evolution is moving from reactive to proactive measures. Just as vaccinations prep an immune system for a foreign pathogen, so too can Threat Intelligence Platforms (TIPs) provide the necessary intelligence to prepare for impending attacks. There has been a fundamental shift in the security industry over the past few years whereby companies are moving away from a reactive model to a more proactive security model leveraging

advances in ML/AI to scale and dynamically tune protective measures. Consequently, a modern TIP that leverages advances in ML/ AI is a necessary resource for protecting space assets in an ever-evolving security environment.

Supply Chain Management

Steve Lee *AIAA*

As discussed at length within this paper, it is crucial to ensure the integrity of constituent components. Most systems, processes, and services are all value-adds: they build upon existing systems, processes, and services. Consequently, there are strong corollaries between the nuclear power industry and space systems. The nuclear industry has a long history of security and integrity of their supply chain. There is no surprise then, that the similarity of demands makes the nuclear power industry's supply-chain security guidance a natural starting point for securing the supply chains of space systems.

On Board Computer Security and Containerization

Dean Hawes & Frank Pound *KubOS & AstroSec*

Protecting large-scale systems on Earth is a known quantity. The difficulties and nuances are well-documented and fairly well understood. One of the core principles of doing so is to assume that, at some point, an attack will succeed and the system will need to be resilient against that attack. In other words, apply equal rigor to protecting against attacks as recovering from successful attacks. Use of Containers and/or Hypervisors to isolate processes and permit rapid recovery is discussed along with appropriate recommendations to bring this same resiliency to space systems.

Quantum Key Distribution

David Mitlyng *Speqtral Quantum Technologies*

As we look to the future, we need stronger encryption distribution protocols to overcome increasingly sophisticated eavesdroppers and hackers. Quantum Key Distribution (QKD), also known as quantum encryption and quantum cryptography, offers a secure solution for distributing encryption keys with the ability to detect the presence of eavesdroppers. Terrestrial use of QKD is currently limited to a range of 100km due to degradation of the signal in fiber-optic cables, leaving Space-based QKD as the best choice for distributing encryption keys and the only secure method of relaying secure keys around the world. The mathematical problems that currently underpin all major encryption methods will not last forever – they're unlikely to last much longer, actually, as quantum computation moves out of the laboratory and into the hands of attackers. QKD is a critical part of the next phase of confidentiality and has already been demonstrated on smallsats and ground systems alike.

Formal Methods for Cyber Resilience

Eddy Westbrook & David Archer *Galois, Inc.*

Software errors or “bugs” pose a real and imminent threat to space systems because they negatively affect reliability and can even cause complete mission failure. This is especially true of security-related software errors, also known as vulnerabilities, because of the high value of space systems as targets of cyberattack and the vast resources that a number of nations around the world are devoting towards developing cyberattack capabilities to target these vulnerabilities. Traditional methods for preventing and mitigating software errors, including testing and code reviews, are of limited effectiveness and do not scale with the complexity of software. Formal methods are one emerging approach that is effective at preventing software errors at scale. The formal methods approach works by analyzing a piece of software and mathematically proving that it is free from errors. The power of formal methods is that these mathematical proofs provide exhaustive coverage of all possible states and execution paths of the software being analyzed and ensure that the software is free from errors. Formal methods thus help make software cyber resilient against both mission failures and cyberattack. In our experience applying formal methods to real-world systems, the key to applying formal methods is to target those software components that are critical to security and mission success. Formal methods should then be integrated into the software development process through the DevOps system to ensure that each new version of the software is free from errors as the software is being developed