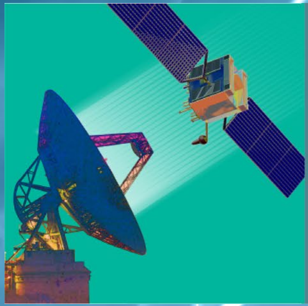
Working Group Session 11G Outbrief



Ground System Architectures Workshop

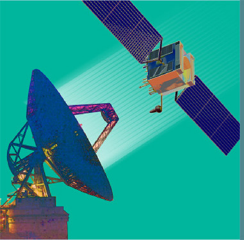
Opportunities in Data Exploitation

March 2–5, 2020 | Renaissance Los Angeles Airport Hotel

Using Data for Novel Approaches in Cybersecurity: Detecting Threats, Reducing Risk and Ensuring Data Integrity

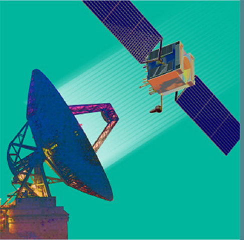
Leads:
Scott Niebuhr and Michelle Yohannes,
The Aerospace Corporation

Approved for public release. OTR 2020-00511.



Session Goals

Present an array of topics to enhance space mission resiliency and highlight current efforts to reduce cyber risks and ensure confidentiality and integrity of data in increasingly connected systems.



Ground System Architectures Workshop

Presenters

Gilles Kbidy, L3Harris Technologies
Secure Ingest: A Common Service approach for implementing secure edge data ingest solutions for Enterprise Ground System Infrastructures

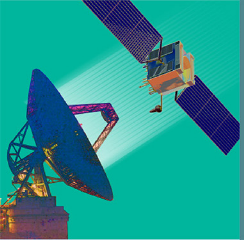
Dr. Pouyan Amirshahi, The Aerospace Corporation
Protecting the Satellite Data Fidelity by Monitoring the RF Spectrum at the Ground Station

Leon Davidson, Oracle National Security Group
Using Blockchain for Imagery Supply Chain Management

Brandon Bailey, The Aerospace Corporation
Re-defining Success of Ground Cyber Assessments

Rafael Martinez, Loyola Marymount University & **Barry Lyons**, KPMG
Interactive discussion on Satellite Cybersecurity

Working Group Session 11G

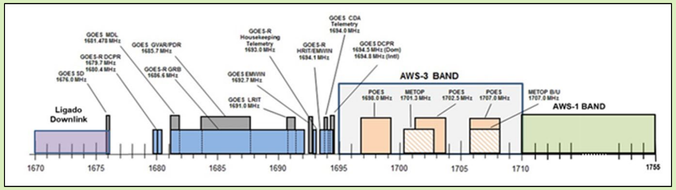


Ground System Architectures Workshop

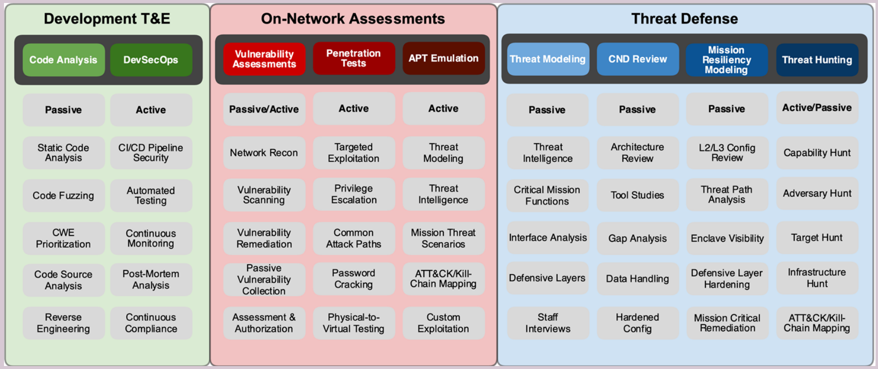
Key Points

Secure Ingest – a novel data validation, edge solution to ensure data integrity in near real time that is tunable based on a high, medium, or low trust source.

Radio Frequency Interference Monitoring System (RFIMS) - Spectrum is crowded and overlapping as DoD and commercial entities share the same radio frequencies.



Cyber Assessments - Move beyond paper compliance to perform holistic testing to include both passive and active assessments with consideration to mission threads and threats.



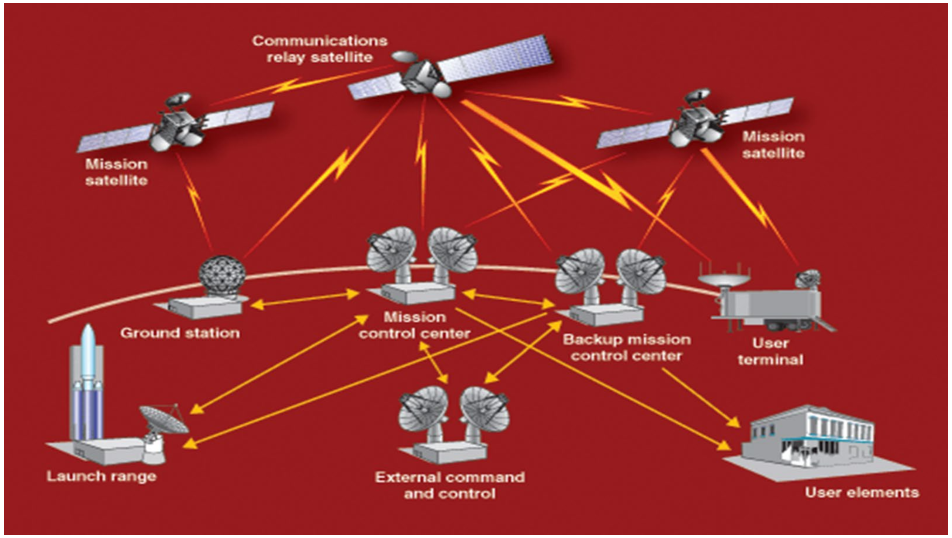
Development T&E		On-Network Assessments			Threat Defense			
Code Analysis	DevSecOps	Vulnerability Assessments	Penetration Tests	APT Emulation	Threat Modeling	CND Review	Mission Resiliency Modeling	Threat Hunting
Passive	Active	Passive/Active	Active	Active	Passive	Passive	Passive	Active/Passive
Static Code Analysis	CI/CD Pipeline Security	Network Recon	Targeted Exploitation	Threat Modeling	Threat Intelligence	Architecture Review	L2/L3 Config Review	Capability Hunt
Code Fuzzing	Automated Testing	Vulnerability Scanning	Privilege Escalation	Threat Intelligence	Critical Mission Functions	Tool Studies	Threat Path Analysis	Adversary Hunt
CWE Prioritization	Continuous Monitoring	Vulnerability Remediation	Common Attack Paths	Mission Threat Scenarios	Interface Analysis	Gap Analysis	Enclave Visibility	Target Hunt
Code Source Analysis	Post-Mortem Analysis	Passive Vulnerability Collection	Password Cracking	ATT&CK/Kill-Chain Mapping	Defensive Layers	Data Handling	Defensive Layer Hardening	Infrastructure Hunt
Reverse Engineering	Continuous Compliance	Assessment & Authorization	Physical-to-Virtual Testing	Custom Exploitation	Staff Interviews	Hardened Config	Mission Critical Remediation	ATT&CK/Kill-Chain Mapping

Blockchain for Imagery Data – Assuring data integrity with through chain of custody.

Working Group Session 11G

Conclusions

- Take a holistic approach – broaden the authorization boundary but operate with zero trust inside the boundary
- Defense in depth- if an adversary breaks through the outside layer, there are more layers of security to get through
- Focus on analysis of mission threads, adversary threats, and system vulnerabilities to determine and implement mitigations.



Its not about risk elimination, its about risk management which requires understanding your mission, the environment (infrastructure, architecture, and boundaries), and the threat.

Working Group Session 11G