Specific Recommendations

Commercial Space System Security Guidelines

Edited by Harrison Caudill & Chris Wake, Orbital Security Alliance

rev-1.0.1 – February 1, 2020

Operational Integrity of TT&C

Karl Mattson *LA Cyber Lab*

Key Recommendations	
Recommendation	**Level**
Adapt and adopt the mandatory security controls recommended by the SWIFT CSP to protect the operational integrity of the Telemetry, Tracking, & Control (TT&C) system.	–

External References	
Reference	**Organization**
SWIFT Customer Security Program[1]	SWIFT

Guidelines for Physical Layer Security

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

Key Recommendations	
Recommendation	**Level**
Be cognizant of the probability of electrical intercept when operating antenna systems.	e.g. Don't do software upgrades from insecure ground stations.
Trust but verify. Only believe what can be proven, and understand that this principle applies equally to networking switches as it does to wireless networking chips.	e.g. Assume inaccuracy in every data sheet, and only believe what you can prove in the lab.
In secure ground stations, employ sophisticated monitoring systems looking for signal anomalies beyond just quality of service.	e.g. Monitor for transmissions that occur before a contact begins, and after it ends.
Utilize a signal spreading technique to guard against impersonation, and possibly also confer jamming resistance.	e.g. DSSS with a chip rate of $\geq$8
Utilize strong encryption on all communications.	e.g. AES 256
While beyond the scope of this section to properly define, it is crucial to ensure strong Network Access Controls are employed to guard the sensitive Radio Frequency systems.	–

info@orbitalsecurity.space

External References	
Reference	**Organization**
Zero Trust Architecture: Draft NIST SP 800-207[2]	NIST
Risk Management Framework[33]	NIST
Spectrum Spreading[3]	Telesat
Application Note 1313 - Testing and Troubleshooting Digital RF Communications Transmitter Designs[4]	Keysight Technologies
The Evolution of Security in 5G[5]	5G Americas

Intelligence: The IoT Crisis

Garry Drummond *802Secure*

Key Recommendations	
Recommendation	**Level**
Discovery – Deploy a wireless Internet of Things (IoT) monitoring system capable of discovering wireless systems over a wide band, passively interrogating to determine device type, and validating the device's configuration against a security policy.	–
Detection – Proactively identify and address unacceptable vulnerability conditions and exposure states prior to loss or incident occurring.	Continually
Response – Integrate wireless monitoring system with general monitoring and response systems (such as Security Incident and Event Management (SIEM) and/or software-defined networking systems).	Able to isolate devices from core network at minimum.

External References	
Reference	**Organization**
The Emerging Cybersecurity IoT Crisis	802Secure

Intelligence: Threat Intelligence Platforms

Chris Adams *ThreatConnect Inc.*

Key Recommendations	
Recommendation	**Level**
Perform a Crown Jewels Analysis of all operational systems and keep that analysis up-to-date.	–
Enumerate assets, infrastructure, and networks identified during the Crown Jewels Analysis and employ appropriate monitoring and controls.	–
Deploy a Threat Intelligence Platform compatible with existing infrastructure.	–

External References	
Reference	**Organization**
Systems Engineering Guide[6]	MITRE
ATT&CK for Industrial Control Systems[7]	MITRE
ATT&CK for Enterprise[8]	MITRE
STIX/TAXII Documentation[9]	MITRE
Diamond Model for Intrusion Analysis[10]	Department of Defense (DoD)

Supply Chain Management

Steve Lee *AIAA*

Key Recommendations	
Recommendation	**Level**
Comply with §11.2 of the Nuclear Energy Institute publication 08-09, *Cyber Security Plan for Nuclear Power Reactors* and/or Nuclear Regulatory Commission Regulatory Guide 5.71.	–
Use Cybersecurity Maturity Model Certification (CMMC) ratings to facilitate vendor selection and risk management.	Minimum of Level 3
Follow NISPOM subguidance (Sections 8-209. 8-212, 8-215, 8-301, and 8-306) for vendor-related cybersecurity procedures.	–

External References	
Reference	**Organization**
Cyber Security Plan for Nuclear Power Reactors[11]	NRC
Regulatory Guide 5.71[12]	NRC

On Board Computer Security and Containerization

Dean Hawes & Frank Pound *KubOS & AstroSec*

Key Recommendations	
Recommendation	**Level**
Ensure process partitioning and isolation on the On-Board Computer (OBC).	e.g. Docker containers with appropriate configuration.
Ensure data is partitioned between processes on the OBC.	e.g. Docker containers with appropriate configuration.
Leverage methods employed by the Cyber Independent Testing Lab to help guide the decision to perform a software upgrade.	Further research required.
Perform attestation at each stage of startup and ensure overall trusted boot regime.	–
Design in a flexible wipe and redeploy strategy from known good scheme.	–
Implement a strong adversarial testing process as part of the SDL. Think like the adversary.	Best Effort
Ensure software implementation includes unit tests and integration tests. This includes an emulation/simulation environment which will allow for high levels of instrumentation and introspection.	e.g. NASA GSC-16720-1 and/or american fuzzy lop

External References	
Reference	**Organization**
Secure Architecture Design[13]	CISA, Department of Homeland Security
Architecting Cybersecurity Into Embedded Systems & Signals[14]	Armed Forces Communications & Electronics Association (AFCEA)
General-Purpose Controls Simulation[15]	NASA
american fuzzy lop[16]	Michał Zalewski
Cyber Independent Test Lab[17]	

Quantum Key Distribution

David Mitlyng *Speqtral Quantum Technologies*

Key Recommendations	
Recommendation	**Level**
Employ Quantum Key Distribution (QKD) for TT&C systems.	Ideally 100% duty-cycle (One-Time Pad (OTP) equivalent).
Employ QKD for less sensitive service links.	1% duty-cycle

External References	
Reference	**Organization**
Quantum Cryptography Demystified: How It Works in Plain Language[18]	ExtremeTech
Explainer: What is Quantum Communication?[19]	MIT Technology Review
Satellite-Based QKD[20]	Optics & Photonics News

Formal Methods for Cyber Resilience

Eddy Westbrook & David Archer *Galois, Inc.*

Key Recommendations	
Recommendation	**Level**
Specify systems with requirements and properties in mind.	–
Design systems with strong boundaries, starting by isolating critical functions whose expected behavior can be described concisely, and where interfaces to other modules can be succinctly described in terms of correctness.	–
Identify which portions of the system should be formally modeled, and which properties of those models should be proven, according to the system specification.	–
Develop formal models and formal specifications of those properties, and then discharge the relevant proofs.	–
Use automated tools to formally verify the production implementation against those formal models.	–
Develop a DevOps mechanism that includes formal-methods capability and CI implementation of formal-methods proofs, just as is done with testing, so that every design change is fully checked and verified against all of the formal models used.	–

External References	
Reference	**Organization**
Continuous Formal Verification of Amazon s2n[21]	Springer Open

References

[1] Swift customer security controls framework. [Online]. Available: https://www.swift.com/myswift/customer-security-programme-csp/security-controls

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Draft nist special publication 800-207, zero trust architecture," NIST, Tech. Rep., 09 2019. [Online]. Available: https://csrc.nist.gov/News/2019/zero-trust-architecture-draft-sp-800-207

[3] "Briefing on spread spectrum technology," Telesat, Tech. Rep., 11 2010. [Online]. Available: https://www.telesat.com/sites/default/files/telesat/files/whitepapers/Spread-Spectrum.pdf

[4] "Testing and troubleshooting digital rf communications transmitter designs," Agilent Technologies, Tech. Rep., 01 2002.

[5] "The evolution of security in 5g," 5G Americas, Tech. Rep., 10 2018. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper-07-26-19-FINAL.pdf

[6] "Systems engineering guide," MITRE, Tech. Rep., 2014. [Online]. Available: https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf

[7] (2020, 01) Att&ck for industrial control systems. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page

[8] (2019, 10) Att&ck enterprise matrix. [Online]. Available: https://attack.mitre.org/matrices/enterprise/

[9] (2019, 08) Cyber threat intelligence technical committee. [Online]. Available: https://oasis-open.github.io/cti-documentation/

[10] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," Department of Defense, Tech. Rep., 05. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

[11] "Nei 08-09: Cyber security plan for nuclear power reactors rev 6," Nuclear Energy Institute, Tech. Rep., 04 2010. [Online]. Available: https://www.nrc.gov/docs/ML1011/ML101180437.pdf

[12] "Regulatory guide 5.71: Cyber security programs for nuclear facilities," U.S. Nuclear Regulatory Commission, Tech. Rep., 01 2010. [Online]. Available: https://www.nrc.gov/docs/ML0903/ML090340159.pdf

[13] Secure architecture design. [Online]. Available: https://www.us-cert.gov/ics/Secure-Architecture-Design

[14] D. Sheets. (2019, 01) Architecting cybersecurity into embedded systems & signals. [Online]. Available: https://www.afcea.org/content/architecting-cybersecurity-embedded-systems

[15] 42: A comprehensive general-purpose simulation of attitude and trajectory dynamics and control of multiple spacecraft composed of multiple rigid or flexible bodies. [Online]. Available: https://software.nasa.gov/software/GSC-16720-1

[16] M. Zalewski. american fuzzy lop (2.52b). [Online]. Available: http://lcamtuf.coredump.cx/afl/

[17] The cyber independent testing lab. [Online]. Available: https://cyber-itl.org/

[18] D. Cardinal. (2019, 03) Quantum cryptography demystified: How it works in plain language. [Online]. Available: https://www.extremetech.com/extreme/287094-quantum-cryptography

[19] M. Giles. (2019, 02) Explainer: What is quantum communication? [Online]. Available: https://www.technologyreview.com/s/612964/what-is-quantum-communications/

[20] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, "Satellite-based qkd," *Optics & Photonics News*, 2 2018. [Online]. Available: Anoptionalnote

[21] A. Chudnov, N. Collins, B. Cook, J. Dodds, B. Huffman, C. MacCarthaigh, S. Magill, E. Mertens, E. Mullen, S. Tasiran, A. Tomb, and E. Westbrook, "Continuous formal verification of amazon s2n," in *30th International Conference on Computer Aided Verification (CAV)*, 2018.

Recommended Reading

[22] H. Caudill, "Big risks in small satellites," Orbital Security Alliance, Tech. Rep., 04 2019. [Online]. Available: https://osa-public.s3.amazonaws.com/papers/big_risks_in_small_sats-v1.0.pdf

[23] B. Bailey, R. J. Speelman, P. A. Doshi, N. C. Cohen, and W. A. Wheeler, "Defending space in the cyber domain," The Aerospace Corporation, Tech. Rep., 11 2019. [Online]. Available: https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf

[24] G. Falco, "Job one for space force: Space asset cybersecurity," Harvard Kennedy School, Tech. Rep., 07 2018. [Online]. Available: https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf

[25] "Challenges to security in space," Defense Intelligence Agency, Tech. Rep., 02 2019. [Online]. Available: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

[26] "Global counterspace capabilities: An open source assessment," Secure World Foundation, Tech. Rep., 04 2019. [Online]. Available: https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf

[27] D. R. Coats, "Worldwide threat assessment of the us intelligence community," Office of the Director of National Intelligence, Tech. Rep., 01 2019. [Online]. Available: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[28] R. Santamarta, "A wake-up call for satcom security," IOActive, Tech. Rep., 2014. [Online]. Available: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

[29] B. Unal, "Cybersecurity of nato's space-based strategic assets," Chatham House, Tech. Rep., 07 2019. [Online]. Available: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf

[30] D. Livingstone and P. Lewis, "Space, the final frontier for cybersecurity?" Chatham House, Tech. Rep., 09 2016. [Online]. Available: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf

[31] T. Harrison, K. Johnson, and T. G. Roberts, "Space threat assessment 2019," Center for Strategic & International Studies, Tech. Rep., 04 2019. [Online]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf

[32] "Cybersecurity maturity model certification - draft," Department of Defense, Tech. Rep., 12 2019. [Online]. Available: https://www.acq.osd.mil/cmmc/docs/CMMC_Version0.7_UpdatedCompiledDeliverable_20191209.pdf

[33] "Risk management framework for information systems and organizations," NIST, Tech. Rep., 12 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf