SSC16-IV-6

Towards Effective Cybersecurity for Modular, Open Architecture Satellite Systems

Presented to:
30th Annual AIAA/USU
Conference on Small Satellites
August 2016

Presented by:
Geancarlo Palavicini Jr.
Daniel E. Cunningham
Jose Romero-Mariona

SPAWAR Systems Center Pacific
53560 Hull Street, San Diego, CA 92152
daniel.cunningham@navy.mil *619-553-3731*

SPAWAR Systems Center PACIFIC

Small Satellite Cybersecurity Challenges

Competing Forces

- Need for rapid system development and fielding
- Desire to leverage low cost technology solutions
- Requirement for information assurance and security

Unique Cybersecurity Challenges

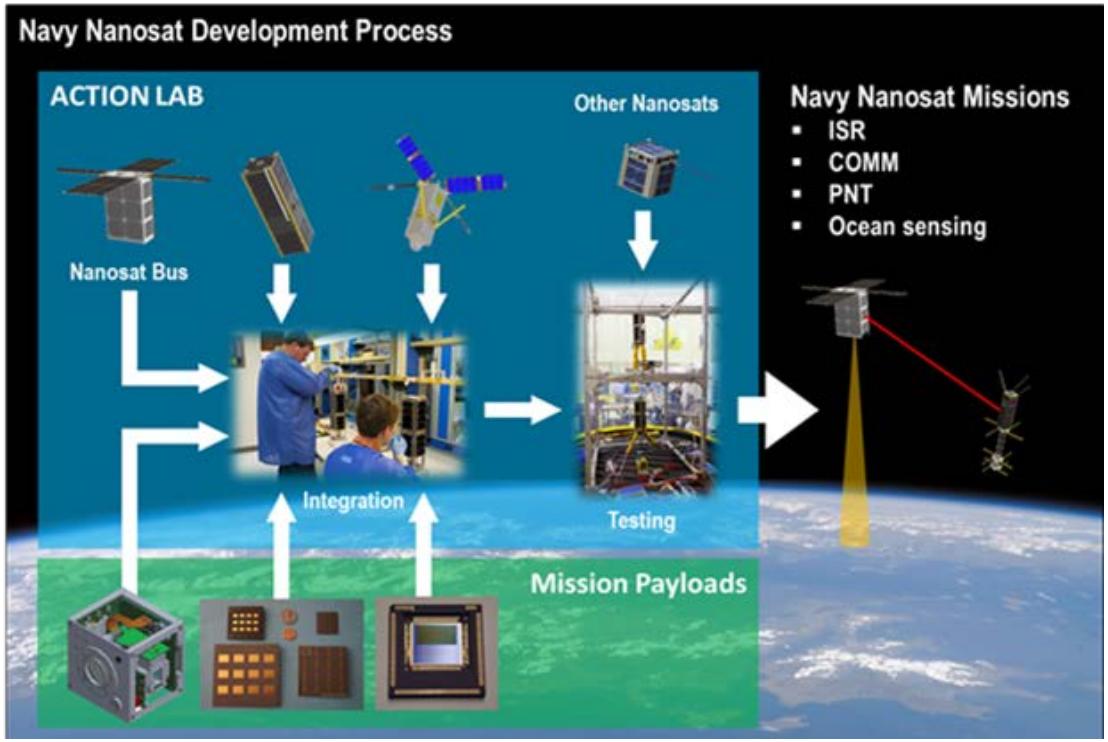
- Inherent risks within low-cost, components-off-the-shelf (COTS)-heavy supply chain
- Modular, net-centric architectures and technologies
- Open-source software products and libraries
- Ground and on-orbit automation
- Time and cost of current space system accreditation processes

Life-cycle Cybersecurity is at Odds with COTS-heavy Plug-N-Play

SSC Pacific Small Satellite Vision

- Government small satellite integration facility
- Rapid prototyping and fielding of responsive space capabilities
- Life-cycle integration and test environment
- Integrate small satellite busses with specialized payloads for military applications
- Infuse cybersecurity into every life-cycle phase
- Leverage specialized resources of government and industry partners
- Break-through traditional space system cost drivers!!

ACCELERATED CAPABILITY FOR TESTING INTEGRATION AND OPERATION OF NANOSATELLITES



SPAWAR Systems Center PACIFIC

Small Satellite Lifecycle Cyber Overlay

Typical Small Satellite Lifecycle	Cybersecurity Overlay
Concept Development & Design	Assess vulnerabilities Plan security controls
Payload & Subsystem Development	Incorporate security controls Greybox and blackbox testing of interfaces
Bus, Payload, & Ground Subsystem Acceptance	Static and dynamic analysis Reverse engineering
System-level Integration and Testing	Dynamic analysis and testing of vulnerability to signal interference, interception, and injection
Launch, On-orbit Operations, and Maintenance	Monitor and defend network & components

SPAWAR Systems Center PACIFIC

Cybersecurity Lab Objectives

- "Test like you Fly" cybersecurity
- Defense-in-depth approach
- Assess security at each layer from the hardware to the network
- Investigate mitigations at each layer
- Penetration testing
  - Dynamic, static & concolic binary analysis
  - Reverse engineering
  - Blackhat techniques to uncover hidden vulnerabilities
- Report on state-of-the-art options for small satellite security
- Recommendations for improving cybersecurity posture

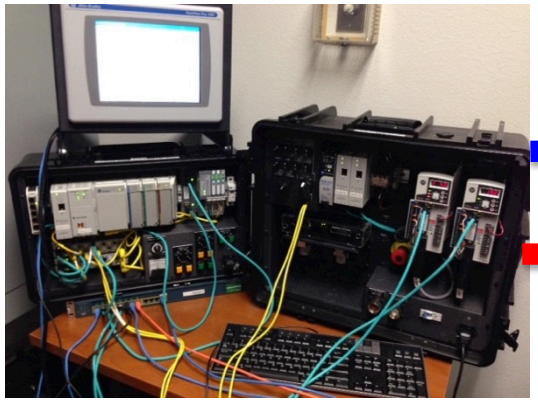
SPAWAR Systems Center PACIFIC

Small Satellite Cybersecurity Hurdles:
Similarities to Industrial Control Systems (ICS)

- CIA vs AIC
  - (C)onfidentiality, (I)ntegrity, and (A)vailability
- Reliance on proprietary protocols and proprietary software for critical operations
- Hardware often constrained in terms of memory & CPU
- Sub-systems often lack proper security testing, thus easily compromised due to large attack surface
- Software updates and patching can be difficult, and slow in implementation
- Lack of manpower that understands both the technology and the cybersecurity

ICS Cybersecurity Methodology for Small Satellites

SPAWAR Systems Center PACIFIC



Vulnerability Scanner

CAULDRON

SCADA Vulnerability Visualization

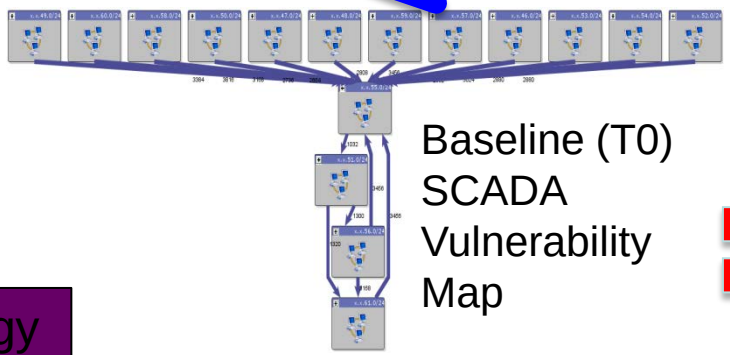
SCADA Data Generation

Rockwell Automation + SIEMENS

Technology X

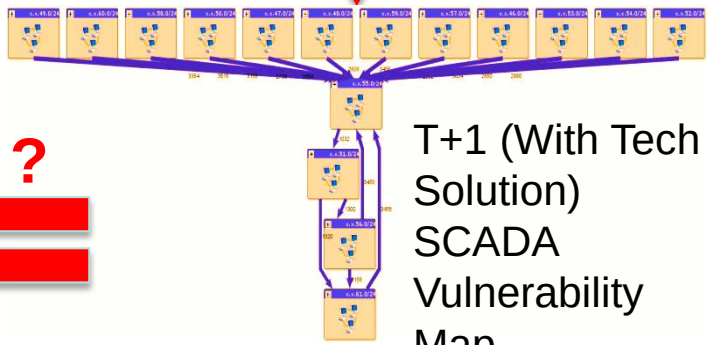
Technology Y

Technology Z



Baseline (T0) SCADA Vulnerability Map

?



T+1 (With Tech Solution) SCADA Vulnerability Map

SPAWAR Systems Center PACIFIC

ICS Cybersecurity Methodology for Small Satellites

- Layered security assessments
  - Hardware -> firmware -> operating system -> user space applications -> network
  - Security controls & mitigations at each layer
- Tools
  - Vulnerability scanners
    - ACAS/OpenVas/nmap
  - Security Assessment
    - Kali Linux / Metasploit
    - Scripting languages – python/ruby/bash
  - Binary Analysis
    - Dynamic, static & concolic analysis (maximize coverage)
    - IDA Pro (Disassemblers for reverse engineering)
  - Continuous security monitoring
    - Sophia (investigating ICS security monitoring tool)

SPAWAR Systems Center PACIFIC

Case Study: Beagle Bone Black

- Network-based vulnerability assessment
  - Limited reconnaissance information gleaned from initial scan
  - Particular test article implemented hardened external interface
- Operating system assessment
  - Linux-based
  - Standard kernel implemented
  - Loadable kernel modules(LKM)
  - Common single-layer defensive approach
  - Lack of OS level hardening
  - No Kernel customization
  - Development tools
- Next Steps
  - User-space application assessments in progress
  - Firmware and hardware assessments in the near future

Geancarlo Palavicini Jr | (619) 553-7904 | geancarlo.palavicini@navy.mil