National Aeronautics and Space Administration

NASA IV&V's Cyber Range for Space Systems

Brandon Bailey

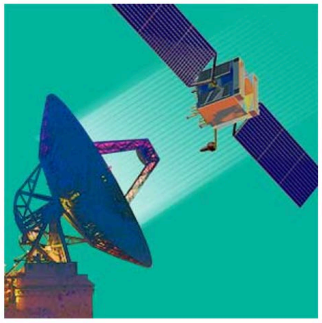
Chief Technology Officer – TMC Technologies

brandon.t.bailey@nasa.gov

brandon.bailey@tmctechnologies.com

304-629-8992

GSAW Plenary
February 2019



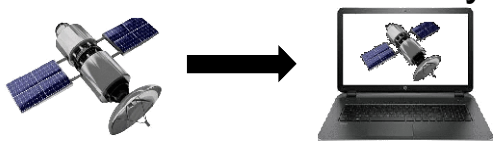
GSAW 2019
Feb. 25-28, 2019

Renaissance Los Angeles Airport Hotel

"Creating Smarter Ground Systems"

NASA IV&V's Lab History

- In 2010, a team of specialized engineers were put together to develop high fidelity simulations to enable dynamic analysis of NASA's spacecraft flight software
  - The Jon McBride Software Testing & Research (JSTAR) laboratory was born out of necessity to enable the development and execution of these simulations
- JSTAR currently contains high fidelity ground to space simulations for many of NASA's most critical missions (i.e. digital twin)
  - GPM, JWST, SLS, MPCV, EGS/GSDO, etc.
  - S/C flight software executes "unmodified" within environments (i.e. a software-only flatsat)



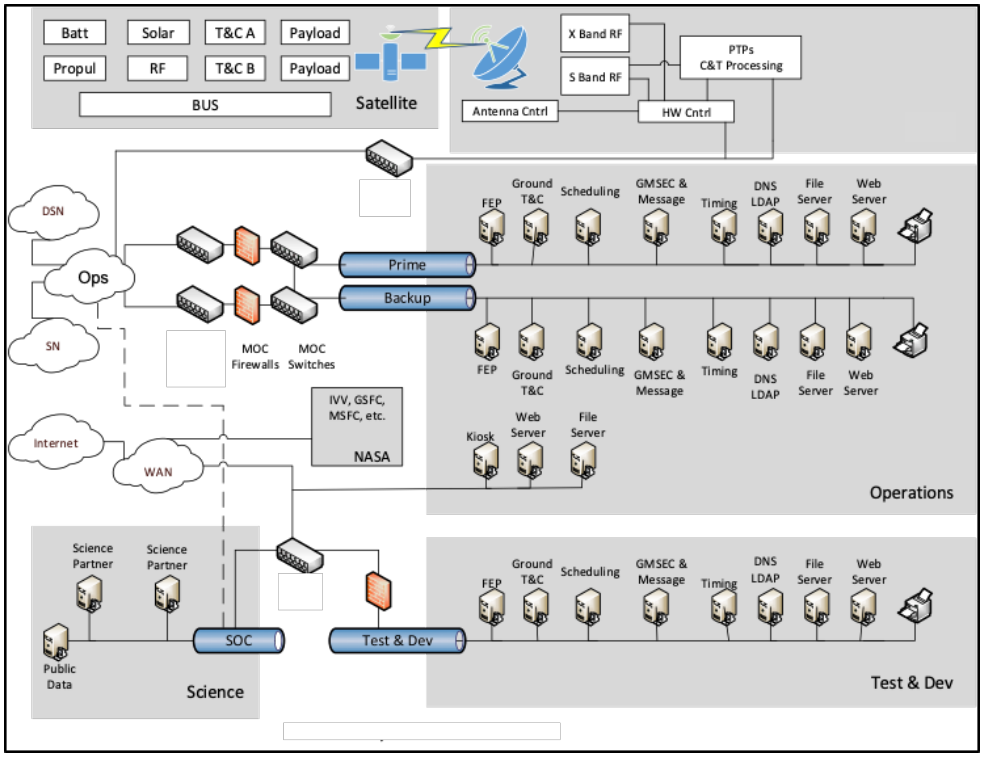
- In 2013, the JSTAR lab's scope expanded to include cybersecurity capabilities (i.e. "cyber range")
  - Ground system cyber assessments (i.e. Blue Team) and penetration testing methodology developed with accompanying training
    - Executed assessments/tests across NASA ground systems for 5 years
- In 2018, combined the high fidelity simulation capability and cyber range with lessons learned from 5 years of assessments on operational ground systems to establish a highly specialized cyber range for space systems

Proof of Concept Completed
End-to-End Virtualized Mission

GSAW 2019

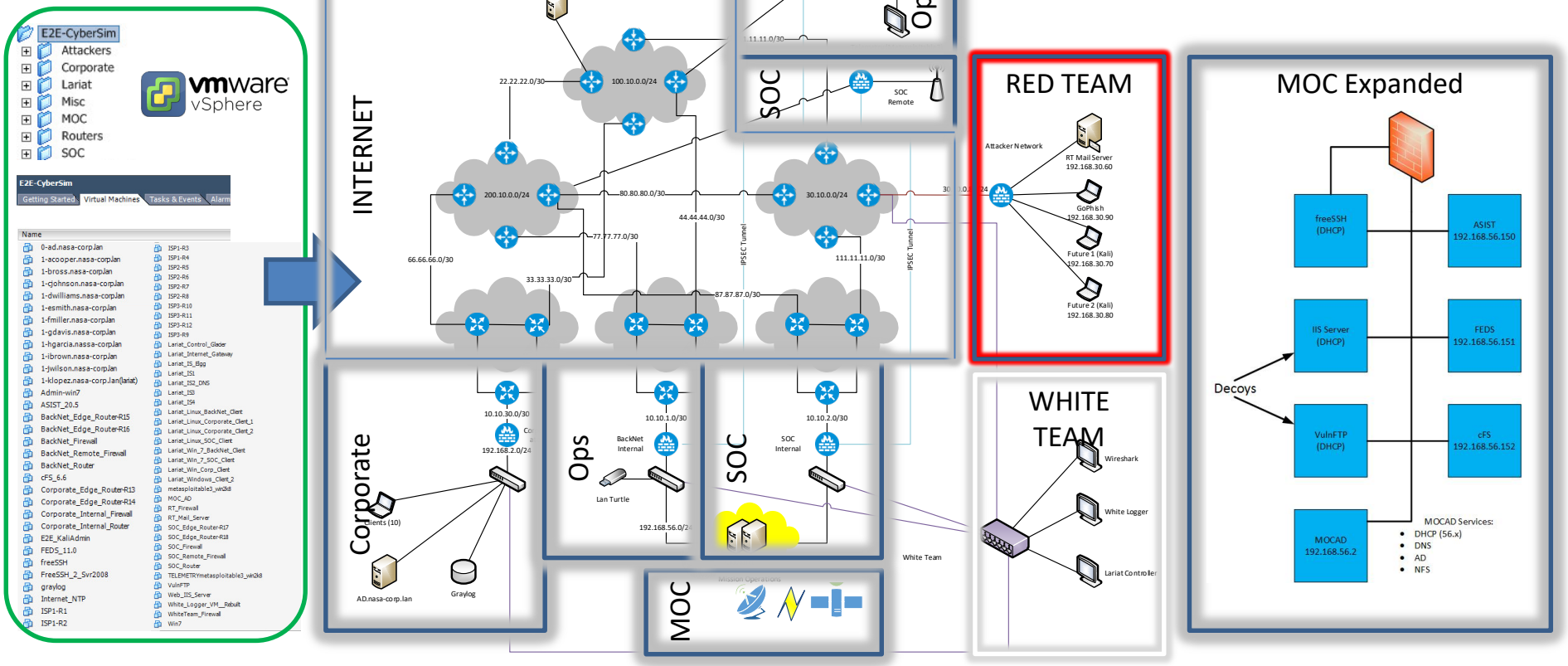
Mission networking environment
- Corporate/Internet Network
- Science Operations
- Mission Ops Infrastructure
- Dev/Test

C&DH environment
- ASIST, FEDS, and cFS
- Built from the ground up
- Bleeding edge SW releases
- Enables plug-and-play into simulations



- A complete Ground System and Satellite packaged in three virtual machines
- Usage of CCSDS Communications Link Transmission Units
- Usage of CCSDS TeleCommand Transfer Frames
- Usage of CCSDS AOS Telemetry Frames
- Ability of ground station to send commands to and receive telemetry from cFS.
- Python scripts that act as 'uplinks' and 'downlinks' and serve to terminate TCP connections to ground and emulate RF transmission to FSW by using UDP.
- CFDP upload functionality from the ground station

Tradecraft Proving Ground



“Capture the Spacecraft” Exercise

- Similar to past Exercises
  - DoD
    - Fallen Angel, Cyber Guard
  - ICS-CERT Training
    - Red vs. Blue
  - But uses all simulation and virtualization to accurately represent real life scenarios
- Red vs. Blue
  - Building on knowledge and principles learned via training
  - 2 Week “live-fire” exercise

IV&V Red Team / Blue Team Training Environment

GSAW 2019

Blue Team Objectives

- Secure the environment: establish baseline, patching, hardening
  - Assets – Firewall, Routers, Windows OS, Linux OS, IDS, DNS Server, Web Application, Database Application, Domain Controller, Web Server
- Detection – After the fact
  - Entry Point Detection – Phish email, Firewall, Routers, Host OS, IDS, Web App, Database App, DC, Web Server
- Prevention – Blocked Intrusion
  - Blocked point - Phish email, Firewall, Routers, Host OS, IDS, Web App, Database App, DC, Web Server
- Incident Response
  - Analyze detection points
  - Ensure environment secured
  - Enforce prevention
  - Trace impact and origin

Red Team Objectives

- Find Vulnerabilities
  - Assets – Firewall, Routers, Windows OS, Linux OS, IDS, DNS Server, Web Application, Database Application, Domain Controller, Web Server
- Exploitation -
  - Assets – Firewall, Routers, Windows OS, Linux OS, IDS, DNS Server, Web Application, Database Application, Domain Controller, Web Server
- Exfiltration
  - Extract “make believe” sensitive data (i.e. Easter eggs)
- Attack
  - The “holy grail” on the attack perspective is to perform the following
    - Send NOOP command to S/C
    - Or run hack.prc script on ASIST
    - Upload custom/malicious TBL or SW to S/C
    - DOS of commanding/telemetry by stopping FEP. “Hack” into the FEP box and kill communication to S/C

- Using the Cyber Range
- Leveraging the Cybersecurity Knowledge Base and Training Curriculum
  - Intro to Cybersecurity and PenTesting
  - ~40 labs
- Intro to Space Systems and Design
  - Ref architectures, ASIST, Front End Data System, CCSDS

Sample Testing Scenarios

- The threat actor would enter the ”enterprise network” or contractor facility via the Internet. Once in, there would be a software development lab (SDL), and the threat actor would have access to an FSW repository of source and compiled and loadable images of the FSW, command & telemetry dictionaries, and sequence. The threat actor objective is to inject malware and/or manipulate that information to hinder the mission in some way.
- The threat actor’s objective would be to deny proper communication with the S/C during a pass. Attacks are launched against ground critical infrastructure where the actor would work to damage/hinder the ability of assets to communicate to the S/C.
- The MOC physical barrier is breached using a lost badge. When the threat actor finds it, this will give them access into the MOC which is coupled with a remote access device. This will garner the threat actor with a persistent remote connection directly into the MOC.

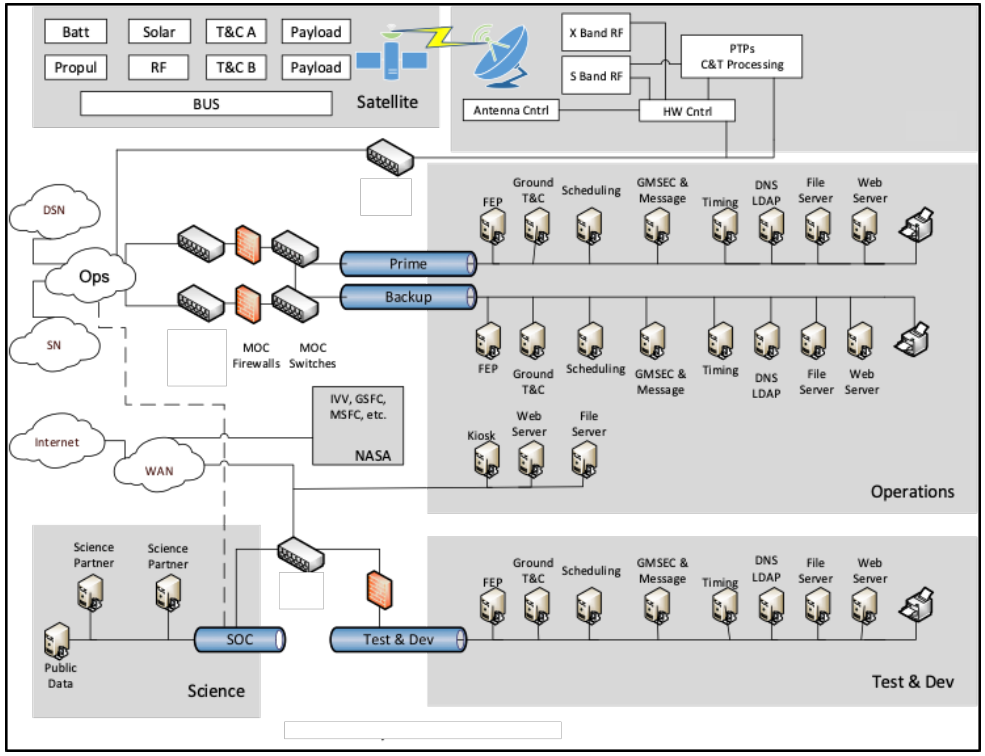
Takeaways from Exercise

- Overall, both teams achieved the scenario objectives
- Blue Team learned to:
  - Detect malicious network traffic
  - Identify adversarial Tactics, Techniques, and Procedures
  - Prevent future attacks by setting security controls
- Red Team learned to:
  - Identify vulnerabilities through network enumeration and testing
  - Exploit vulnerabilities by leveraging pen-testing tools
  - Navigate spacecraft infrastructure
- Infrastructure team took away many lessons learned to better expand and improve realism for future years
  - Improve traffic generation realism relative to each enclave
  - Add spacecraft simulation visualization to enable kinetic effect
  - Malicious 3rd party / Man-in-the-Middle attack
  - ICS/OT integrations (e.g. Tofino, Allen-Bradley, HMI, etc.)
    - Physical or software based ICS systems within the network at various points with defined support and potential cyber-physical

Usages Outside of Red/Blue

- Help ensure the **success of the Mission Objectives** and related capabilities
- Assure the **cybersecurity characteristics and elements** as defined in the planning, development, design, launch, sustained operations, and decommissioning of
  - Space systems and related SW components used to collect, generate, process, store, display, transmit, or receive
  - Supporting and related infrastructure

- Gain knowledge and understanding of the current and projected full range of **threats** to systems and SW
- **Risk informed** decision making
- Increased **assurance** and **resilience** of mission-essential functions and defined capabilities of mission systems, infrastructure
- Help **protect against** disruption, degradation, and destruction, whether from environmental, mechanical, electronic, software, or hostile faults/anomalies



Goal: Environment to support end to end Cybersecurity Assurance (e.g. DT&E)

Plug and Play: JSTAR Simulation Warehouse

GSAW 2019

Human Exploration

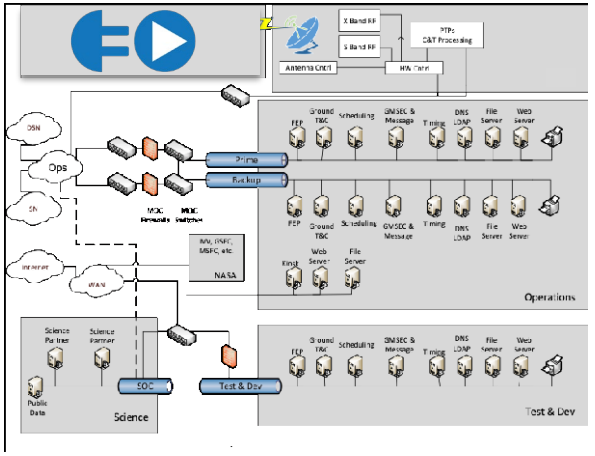
Mission	Platform
Space Launch System (SLS)	SLS Software-only Simulator (S3)
Ground System and Data Operations (GSDO)	GSDO Software-only Simulator (G2)
Multi-Purpose Crew Vehicle (MPCV)	Software-Only Crew Exploration vehicle Risk Reduction Analysis Test Environment Simulation (SOCRRATES) *
Integrated Tri-Program Simulation	Advanced Risk Reduction Integrated Software Test and Operations Tri-program Lightweight Environment (ARRISTOTLE)
International Space Station (ISS)	MADE Final Qualification Tests (FQTs) *

Small Satellites

Mission	Platform
Simulation-to-Flight 1 (STF-1)	NASA Operational Simulator for Small Satellites (NOS^3)
Lunar Ice Cube	

Science Missions

Mission	Platform
JWST	JWST Integrated Simulation & Test (JIST)
DSCOVR	Mission Test Set (MTS)
GPM	GPM Operational Simulator (GO-SIM)
OSIRIS-Rex Insight MAVEN	SoftSim (Lockheed Martin) *
ICESAT-II	ATLAS FSW Simulation Environment *
WFIRST	Leon-4 Emulator, cFS, ASIST, 42, WFI/CGI simulator
Europa	RAD750 Emulator, CORE, GDS, WSTS



*Acquired Simulations