Space Situational Awareness - When is an Anomaly an Attack?

Dave LaVallee, Sam Fix, Brian Garofalo, Steve Parr
JHU/APL

SpaceOps Workshop June 11-13, 2013
Agenda

- Problem Statement
- Objective
- Approach
- Current Status
- Benefits
Cyber Attacks

- Anomalies occur within spacecraft systems: hardware failure, software bug, link interference, sensor failure, etc.
- Could also be an intentional attack by an adversary: jamming, commanding spacecraft or ground system, disabling functionality, modifying or copying data from the control center, etc.
- Need to determine the cause of the anomaly and plan a course of action to return to nominal service (if possible)
- Documented occurrences of cyber attacks:
  - NASA’s TERRA AM-1 spacecraft in June and October 2008
  - LANDSAT-7 spacecraft in 2007 and 2008
  - Both were reported to be taken control of for several minutes
  - ”The responsible party achieved all steps required to command the satellite” according to US-China Economic and Security Review Commission
Space Situational Awareness

Mission Operations Center

Enhanced On Board Situational Awareness

Command Workstation
Telemetry Archive
...Others

Situational Awareness Analysis System (SAAS)
Objective

• Improve space situational awareness onboard and in mission operations centers

• Provide both a fault management and cyber awareness capability

• Give mission operations a quick and easy way to assess the health of a space system (ground, spacecraft, constellation, etc.)

• Give mission operations a simulation tool to see the effect of a fault in the system and what mission components would be affected

• Leverage analytic approaches developed at JHU/APL to do the analysis
Approach

• Investigate possible/plausible attacks

• Prototype telemetry mining application

• Monitor network traffic into and out of the Mission Operations Center

• Create models for analysis and displays for monitoring

• Test using an existing flight software (FSW) testbed
  ➢ Includes “What if?” analysis capability
Current Status

- Visualization Tool
  - Model of an operational system has been refined
  - Ability to base entity status on user-defined functions – think redundant subsystems (if...and...or)
  - Ability to use multiple overlays to support time or phase-based dependencies
- System Drilldown Visualization
  - System Insight (SI) – combines system block diagram, network diagrams, 3D physical views, etc.
  - Have many of the different views of the system defined
- Network Monitoring
  - Configured prototype sensor in FSW testbed network to collect cyber data
  - Monitoring all Mission Operations Center network traffic
Visualization Model – Show Dependencies
Space System Top Level View

Mission Operations Center
Drill Down to MOC View

- Telemetry Clients
  - For sims and launch day
- STK/CDTK Primary/Backup
  - MAX
- HIL Simulator (EM EIM)
- HIL Simulator (EM BB 2)
- HIL Simulator (Flight Spare)
- Mission Telemetry Archive (RAID Array)
- Telemetry/ Raw Archive
- Data Retrieval/Assessment
- MOC File Server
- Telemetry/ Raw Archive
- Data Retrieval/Assessment
- Planning/Scheduling
- Database Server
- SOC Cmd Acceptor
- MOC Data Server
- Spare Server

OPS Network

Commanding Network

Disaster Recovery Network

Instrument SOCs @ Home Campuses
(Internet)
Computer Drill down to Ground Software

- Raw Archiver Service
- Telemetry Service
- Hardware Manager Service
- Commanding Service
- Control Center Software
- Bridge Service
- Archive Manager Service
- Failover Service
- Procedure Platform Service
Network Monitoring – Tool

Network Diagram:
- Development Network
- Testbed Network
- Ops Network
- Command Network
- SOC
- APL
- APL

Diagram Details:
- Nodes
- Links
- Compositing
- Cores
- Clusters
- Bars
- Sequencing
- Test
Network Monitoring – Node Details

**Development Network**

**Testbed Network**

**SOC**

**Command Network**

**Ops Network**
Network Monitoring – Link Details

- BytesFrom: 15132198 (15132198)
- BytesTo: 3124580 (3124580)
- BytesTotal: 18256778 (18256778)
- EntropyFrom: 250 (250)
- EntropyTo: 250 (250)
- LinkColor: Gray (Gray)
- PacketsFrom: 0 (0)
- PacketsTo: 0 (0)
- PacketsTotal: 0 (0)
- PortFrom: 58003 (58003)
- PortTo: 57097 (57097)
- Protocol: TCP (TCP)
- Represents: 1
- Sensor:
- SensorLoc:
- TimeStampLast: 2013/06/03 16:10:19 (2013/06/03 16:10:19)
- TrafficType: unknown (unknown)
- UniqueID: 1096
- Weight: 1.0

*Right-click to change hover text settings*
Benefits

• Enable space system operators to monitor for anomalies in the space segment, link segment, ground segment, and network

• Alert operators to symptoms of potential cyber attacks

• The framework can be adapted for new missions

• The models and analytical tools can be easily extended for additional types of attacks

Adds an important new dimension to situational awareness!