Theme Summary: Countering Security Threats to Space Flight & Ground Systems

Pierre Lods, Shinichi Nakamura, Steve Parr, Bill Van Besien

2013 Space Operations Workshop
June 12, 2013

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Countering Security Threats

- Oversight
- Guidance
- Manage Risk
- Secure Practices
- Strong Controls

- Adding security to legacy systems
- Replace crunchy outside, soft inside with
  - Layered Security
  - Defense in Depth
  - Make the center more chewy

Securing Ground Systems

- Security Infrastructure
  - User Management
  - Log Server
  - Screen Lock
  - Application Security
- Encryption, Authentication
- Key Management

- Impact on performance

Information Security Management System IT Security

- ISO 2700[0,1,2,5]
  - ISO/IEC 27000:2009, Information security management systems — Overview and vocabulary
  - ISO/IEC 27001:2005, Information security management systems — Requirements
  - ISO/IEC 27005:2011, Information security risk management
- NIST Standards SP 800 series
  - NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments
  - NIST SP 800-39, Managing Information Security Risk
  - NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
  - NIST SP 800-61, Computer Security Incident Handling Guide
  - NIST SP 800-64, Security Considerations in Information System Development Life Cycle

Security Policy / Info and Comms Security

- DLR / German Space Operations Center
- ESA Mission Operations Infrastructure

- ISO 27001
- Space Segment
- Ground Segment
- Interoperability of Ground Segments
- Keep documents up to date
- Live the documents
- Continuous Security Improvement

- Is it too much overhead?
  - Integrate with Quality System?
  - Cost of doing / Cost of not doing

Secure Software Engineering

- The last line of defense
- Secure Software Development Lifecycle (SSDLC)
- Generic Application Security Framework
- Requirements
  - Functional
  - Assurance
- Confidentiality/Integrity/Availability

Space Link Security

- EUMETSAT and ESA

- Encryption / Authentication
- Cost / Benefit / Risk
- Space Mission Security Architecture
- Data Link Layer
  - CCSDS Space Data Link Security (SDLS) protocol
- Physical Layer
  - Spread Spectrum Modulation
  - Direct Sequence Spread Spectrum CDMA Enhancements

Security Primitives for Packetized Data Links

- Using CCSDS DTN Bundle Protocol
- Simplified Bundle Security Protocol
- Packetized Data
- Multi-Hop
- Multi-Path
- DTN Overlay network
- Focus on End to End
  - Integrity, Confidentiality
  - Decouple Routing from Security
- Encapsulation
- Deployment Considerations

Space Situational Awareness / Metrics

- Visualization
  - Layered model with dependencies
- Drill down from S/C to MOC and Ground Software
- Network Monitoring

- How do you measure system and mission effectiveness?
- Mission Essential Functions
- Use Cases
- System Measures of Effectiveness
- Mission Measures of Effectiveness
- System Model and Evaluator

Theme Summary

- Security requirements are not going away
  - They are increasing substantially
  - They are likely to be with us for a long time
- We have to adapt legacy systems
- Security should be incorporated at the system level
  - Ground, Space, Link
  - Interoperability will grow
- We have to engineer our software and our systems with security in mind
- We have to do this without additional budget