Cybersecurity Risk Analysis (and Resiliency) of Satellites

Daniel D. Doyle, PhD
Research Assistant Professor
Aerospace and Ocean Systems Lab
Hume Center for National Security and Technology
Space Situational Awareness

SOSI, proximity operations, and tracking

Resilient Mission Platforms

Robust and secure control of platforms and payloads

Autonomy and Mission Orchestration

Distributed, cross-layer cognitive management engine

Cubesats and Small Satellites

Satellite ground station and cubesat launches

Representative Programs

SquadX
Core Technologies & Experimentation
Autonomous control of EM battlespace to combat adversary UAS platforms

Hallmark
TA1: Tools/Technology
SOSI situational awareness in degraded or denied sensing environments

NAVAIR
Airworthiness Center
Cybersecurity in airworthiness, failure modes, criticality, and common criteria

Code 32
Low-SWAP EW Payloads
Low-power GPU platforms for cognitive EW missions, leveraging SDR and deep learning
Scalable Autonomy / Third Offset

Scalable Autonomy

I & W → Tracking → Prediction → COA Recommendation → COA Selection → COA Prosecution

Optimal/Adaptive Controls → Adaptive Configurability and Mission Management → Machine Learning and Data Fusion

Cognitive Management Engine

Search → Cognitive Mgmt Engine → Survey → Recon → Missions → Targets → Compute → RF Resources → Optimize
• Rate of commercial, small satellites being launched is growing significantly
• SpaceX and OneWeb alone are planning to launch thousands of satellites for their space-based Internet platforms and represent a new inflection point
• Major research challenges and opportunities
  • Affordable satellite, payload, and launch technologies
  • Scalable and resilient command and control
  • “Air traffic control” in increasingly dense low-earth orbit

Cybersecurity Vulnerabilities, Mitigations, and Resiliency

Vulnerabilities
• Research and compile lessons learned and pertinent information
• Perform a cyber risk assessment

Mitigations
• Analyze data and assessment to provide a common understanding of risks associated with SmallSats
• Develop techniques and strategies for mitigation

Resiliency
• Provide a model-based systems engineering approach towards developing resiliency
Related Work - Research & Innovation

• Small Satellite Design and Manufacturing Lab
  • Optimal / adaptive design and manufacturing
    • Space@VT
    • Industrial Systems Engineering/Center for High Performance Manufacturing
  • Interdisciplinary Center for Applied Mathematics (ICAM)
  • Advanced Manufacturing Team
• VT ground station for data fusion / analytics research, ground processing, and hands-on education
• Reconfigurable autonomous payloads
• DISCO optimal space mission design
• Successful startup and prime contractor partnerships

• Developing and licensing wireless avionics
Related Work - Launches!

Student Payloads

- 5 Launches in 2017
- 8 planned in 2018

Research Missions

- Cybersecurity Risk Analysis (and Resiliency) for Satellites

Figure F3. The SOCRATES observatory. The +X direction provides the instrument solar occultation view.
Experimental Plan

- Develop an understanding of the most common SmallSat cybersecurity risks
  - Review previous and current work / literature review
  - Use NIST Framework for Improving Critical Infrastructure Cybersecurity

- Modeling and Threat Exercise
  - Use in-house SmallSat and Multi-rotor research as testbeds
  - Characterize ways to attack dynamic cyber/physical systems
    - Check physical degradation, injection noise – controllability of the system
    - Change clock parameters for sparse control inputs – frequency changes
    - If encryption not applied... what happens
    - If commands captured... can they decode, match, etc.
  - Apply ways of physical access to code / transistor that accesses BIOS
  - Apply GPS spoofing
  - Inject malicious commands

- Define and provide a common understanding of risks and vulnerabilities associated with SmallSats

- Develop and understand mitigation strategies that would refine approach in providing opportunities or best practices that customers could use as a tool for increasing cybersecurity resiliency
Milestones/Deliverables

NOV 2018–FEB 2019
- Research/Compile Lessons Learned

MAR–MAY 2019
- Cyber Risk Assessment

JUN–AUG 2019
- Mitigation Strategies
  - NIST Cyber Framework
  - Threat Modeling Exercise
  - Strategies List

SEP–NOV 2019
- Publish

IN-HOUSE EXPERIENCE

LESSONS LEARNED REPORT

DATABASE

1. Identify information assets.
2. Locate information assets.
3. Classify information assets.
   1. Public information
   2. Confidential sensitive information
   3. Sensitive internal information
   4. Comparted sensitive internal information
   5. Restricted information
4. Conduct a threat modeling exercise.

STEPS:
- Scoping of Identity
- Temporal with Data
- Replication of Transactions
- Information Extraction
- Denial of Service
- Elevation of Privilege
- Finalize data and effort planning.

Cybersecurity Risk Analysis (and Resiliency) for Satellites
11/14/2018
Benefits to Society

• These autonomous wireless architectures are inherently vulnerable to network degradation and failure in the form of malicious and unintentional cyber incidents
  • Producing a set of vulnerabilities and mitigation strategies enables a checklist of sorts for ensuring safer and more resilient SmallSats
  • Using the list of vulnerabilities and mitigations has the potential to ensure safer, resilient SmallSats providing customers with needed confidence
  • As companies seek to launch thousands of these SmallSats, mitigating cybersecurity risks are imperative
Thank you for your support!

danieldoyle@vt.edu, jonathan.black@vt.edu, kschro1@vt.edu

www.hume.vt.edu/research/aero
www.space.vt.edu
www.aoe.vt.edu
References

- http://stuffin.space/
- https://www.nasa.gov/centers/ivv/services/cybersecurity_risk.html - Risk Assessment
- https://www.meritalk.com/articles/how-vulnerable-are-u-s-satellites-to-cyberattacks/
- https://lifelinedatacenters.com/data-center/cyber-attacks-on-satellites/