CubeSAT Cybersecurity Challenge

AIAA Aerospace Cybersecurity Working Group
DEF CON 29 Aerospace Village, August 6-7

Copyright © by aiaa.org
Published by the American Institute of Aeronautics and Astronautics, Inc., with permission.
Contributors

- Arun Viswanathan, Jet Propulsion Laboratory, California Institute of Technology
- Andrew Santangelo, SciZone
- Gregory Falco, Stanford University
- Jeremy Straub, NDSU
- Michel Ingham, Jet Propulsion Laboratory, California Institute of Technology
- Steve Lee, AIAA
Introduction to the Session

- **Workshop Objectives**
  - Interactive content like this event and the table top exercise are key to AIAA's aerospace cybersecurity strategy
  - A best practice in cybersecurity—and in aerospace

- **What this workshop is about?**
  - A learning—not competitive—activity
  - Primarily cultivation of technological cybersecurity skill—but also the people and process skills for cybersecurity to succeed
Agenda

- **Introduction to the session – 5 Minutes**
  Steve Lee – AIAA

- **Section 1: CubeSAT 101**
  Andrew Santangelo, SciZone

- **Section 2: Attack Methodology – Think Like a Hacker**
  Greg Falco, Stanford University

- **Section 3: Attacking CubeSATs - Live Interactive Session + Demo**
  Greg Falco, Stanford University
  Arun Viswanathan, Jet Propulsion Laboratory, California Institute of Technology

- **Section 4: Thoughts on Mitigations**
  Open discussion

- **Section 5: Lessons Learned and Conclusions**
  Open discussion

- **Section 6: Homework Hackathon (open to all)**
  Open discussion

- **Final Thoughts, Conclusions and Q&A**

  - 5 minutes Q&A after section 1, 2 and 3
  - Please use the chat to ask questions
  - Links to Zoom Sessions (8/6, 8/7) and session handouts are located at https://aerospacevillage.org/aiaa-cubesat-hacking-workshop
Section 1: Cube/Small SAT 101
Situational Landscape

- Scientific Missions
- Military Operations
- Education Missions
- Commercial Enterprise
- Civic Operations
- Hobbyists
CubeSat/Small Satellite Market Size

### SmallSats Wet Mass

- **Pico-Satellite**: < 1 kg
- **Nano-Satellite**: 1 – 10 kg
- **Micro-Satellite**: 10 – 100 kg
- **Mini-Satellite**: 100 – 500 kg

Cubesat growth >1,400 units/year by 2022
Mini-satellite Growth >250 units/year by 2022

Sample of CubeSat/SmallSat Missions

MarCO Cubesats

AUBURN TRYAD Mission

Asteria

HSFL Neutron-1 Mission

LinkStar-D Duplex Radio Antenna

Carthage College CaNop Mission

LinkStar-D Duplex Radio

NRL Cubesat
Components of a CubeSAT

Components of A Generic Space System

1. As defined in, Memorandum on Space Policy Directive – 5 Cybersecurity Principles for Space Systems, Sep 2020
sci_Zone LinkStar-QuickSAT Architecture

- FRNCS-P flight computer & QuickSAT/VMS
- SCADA Terminal
- SCADA store/forward device
- Data Port
- Control Port
- Remote DTE

Rx  Tx
Antenna

Globalstar Gateway

AWS, AWS Gov Cloud, or Other Cloud Based Servers

Host Server

QuickSAT/VMS or other server
Components of **LinkStar Architecture**

- **LinkStar-TRK**
- **LinkStar-D**
- **LinkStar-HD**
- **S-Band/X-Band**

**QuickSAT**

- Xilinx Zynq UltraScale MPSoC
- Flight Computer

**Other Computers**

- QuickSAT Power Management
- 0.5U form factor
- 1-4W
- Watchdog timers and external signal reset
- Hypervisor

**OEM-719, ADA Fruit UltimateGPS**

**GPS**

**Sensors**

**Actuators**

**Components of LinkStar Architecture**

- LinkStar-TRK
- LinkStar-D
- LinkStar-HD
- S-Band/X-Band
- QuickSAT
  - Xilinx Zynq UltraScale MPSoC
  - Flight Computer
- Other Computers
  - QuickSAT Power Management
  - 0.5U form factor
  - 1-4W
  - Watchdog timers and external signal reset
  - Hypervisor
- OEM-719, ADA Fruit UltimateGPS
- GPS
- Sensors
- Actuators
SciZone *QuickSAT* Architecture

- **Broad Use:** Aviation, Satellites, Cars
- **A complete Flight Management System**
- **Vehicle Health Management & Monitoring**
- **Vehicle Commanding Services**
- **Communications services**
- **Test/Monitoring interface**
- Can serve as a stand alone ground station or part of an expanded environment
- **Customizable**
- Utilizes open source software where possible
- Works on a range of flight hardware
- Web based Interface - PCs, Tablets, etc.
CubeSATs are IoTs in Space!
IoTs in Space: *LinkStar-QuickSAT* Example

Globalstar™ Satellite

Globalstar™ Ground Station

sci_Zone™ Servers

Customer Mission Control

sci_Zone, Inc.
www.sci-zone.com
Space Systems are Vulnerable to Cyber Attacks

ROSAT X-Ray Attack - 1998
Since 2007, several elite APT groups have been using — and abusing — satellite links to manage their operations — most often, their C&C infrastructure, for example, Turla.

**Black Hat 2020**: Eavesdropping on Sat ISPs. Basically, ISP not protecting their links and it can be picked up easily.

**June/July 2008**: Terra EOS AM-1/Landsat-7, attempted satellite hijacking, hackers achieved all steps for remote command of satellite.

**2013-2014**: UT Austin Radio Navigation Lab conducts GPS spoofing for UAV control and navigation interruption.

---

3. Turla APT Group Abusing Satellite Internet Links, Threatpost, Sep. 2015
6. UT Austin Radio Radionavigation Laboratory
Section 2: Attack Methodology
# High-Level Threats Against Satellites

<table>
<thead>
<tr>
<th>Threat</th>
<th>Applicability</th>
<th>Description</th>
<th>Impact Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized control</td>
<td>Space segment, ground segment</td>
<td>A type of threat action whereby an entity assumes unauthorized logical or physical control of a system resource</td>
<td>Adversary assumes remote control of a spacecraft, or ground systems.</td>
</tr>
<tr>
<td><strong>Corruption / modification of system and/or data</strong></td>
<td>Space segment, ground segment, Link segment</td>
<td>A type of threat action that undesirably alters system operation by adversely modifying system functions or data. Subtypes: “tampering,” “malicious logic,” “hardware/software error”</td>
<td>A corrupted spacecraft command could result in catastrophic loss if either no action occurred (e.g., command is discarded) or the wrong action was taken onboard a spacecraft.</td>
</tr>
</tbody>
</table>

Adapted from CCSDS 350.1-G-2 Security Threats Against Space Missions
# High-Level Threats Against Satellites

<table>
<thead>
<tr>
<th>Threat</th>
<th>Applicability</th>
<th>Description</th>
<th>Impact Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interception of data</strong></td>
<td>Space segment, ground segment, space-link communication</td>
<td>A type of threat action whereby an unauthorized entity directly accesses sensitive data while the data is traveling between authorized sources and destinations. Subtypes: &quot;RF analysis,&quot; &quot;wiretapping,&quot; &quot;theft&quot;</td>
<td>Interception of data may result in the loss of data confidentiality and data privacy if the data is not encrypted.</td>
</tr>
<tr>
<td><strong>Jamming</strong></td>
<td>Space segment, ground segment, space-link communication</td>
<td>A type of threat action that attempts to interfere with the reception of broadcast communications. Adversary can deny RF communications to/from spacecraft by injecting noise, by transmitting on the same frequency from another source, or by simply overpowering the original source.</td>
<td>Spacecraft commanding as well as the ability to receive science or engineering data from the spacecraft could be blocked. Authorized access may be impacted.</td>
</tr>
</tbody>
</table>

Adapted from CCSDS 350.1-G-2 Security Threats Against Space Missions
## High-Level Threats Against Satellites

<table>
<thead>
<tr>
<th>Threat</th>
<th>Applicability</th>
<th>Description</th>
<th>Impact Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial-of-Service</td>
<td>Space segment, ground segment</td>
<td>The prevention of authorized access to a system resource or the delaying of system operations and functions.</td>
<td>Consumption of resources (e.g., communication bandwidth, processor bandwidth, disk space, memory), disruption of system/network configurations (e.g., routing changes), disruption of state information (e.g., persistent network connection resets), disruption of network components (e.g., router or switch crashes), or obstruction/destruction of communications paths.</td>
</tr>
<tr>
<td>Masquerade</td>
<td>Space segment, ground segment</td>
<td>A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity.</td>
<td>If an external entity can masquerade as a spacecraft operator; unauthorized commands could be transmitted to the spacecraft resulting in damage, data loss, or loss of a mission.</td>
</tr>
</tbody>
</table>
## High-Level Threats Against Satellites

<table>
<thead>
<tr>
<th>Threat</th>
<th>Applicability</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Replay</strong></td>
<td>Space segment, ground segment, space-link communications</td>
<td>An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and retransmits it, possibly as part of a masquerade attack.</td>
<td>If the replayed commands are not rejected, they could result in a duplicate spacecraft operation such as a maneuver burn or a spacecraft reorientation with the result that a spacecraft is in an unintended orientation.</td>
</tr>
<tr>
<td><strong>Software threats</strong></td>
<td>Space segment, ground segment</td>
<td>Misconfigurations, programming errors, installation of malicious/unvetted software, and exploitation of vulnerabilities by threat agents.</td>
<td>Loss of data, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.</td>
</tr>
</tbody>
</table>
## High-Level Threats Against Satellites

<table>
<thead>
<tr>
<th>Threat</th>
<th>Applicability</th>
<th>Description</th>
<th>Impact Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply Chain</td>
<td>Space Segment, Ground Segment</td>
<td>Attack in which extra electronic/electrical components to Printed Circuit Boards (PCBs) schematics or layouts. Malicious firmware is added to embedded systems’ microelectronic devices</td>
<td>Covert control of the power controller of the system management bus (SMBus) of a PCB would allow a threat agent to interfere with the communications of ground segment systems and space system sensors.</td>
</tr>
</tbody>
</table>
Introduction to Attack Trees

- Start with a Goal
- Ask yourself “how”?
- Establish sub-goals (branches)
- Ask “how” again
- List the mechanisms to achieve the sub-goal (leaves)

- Think about concurrent requirements (AND Statements)
- Think about alternative paths (OR Statements)
Attack Tree Template

Attacker Goal

When in the attack process?
- Reconnaissance (gather info)
- Weaponization (prepare the weapon)
- Deliver (get the weapon to target)
- Exploit (get into the system)
- Control (manage the system)
- Execute (achieve primary goal)
- Maintain (persistence)

Where do you attack?
- Attack Surface (e.g. web interface, user, administrative panel, etc.)

What is the action?
- Action (e.g. gain access, collect, edit, delete, etc.)

How do you achieve the action?
- Tools
CubeSAT User Interface Demo Video
Section 3: Attacking CubeSATs - Generating Attack Trees for CubeSATs

Interactive Session
Sci Zone **LinkStar-QuickSAT Architecture: Review**

- **QuickSAT/VMS** is the web based interface.
- Communication is via "bent-pipe" to the ground.
- Architecture supports a range of radios including the **LinkStar-TRK** (simplex) and **LinkStar-D** (duplex) plus S-Band, etc.
- The satellite "pushes" and "pulls" data to and from the ground. The ground terminals cannot push data to the satellite.
Interactive Attack Tree Generation
Section 3: Attacking CubeSATS - Demo
Demo Scenarios

- **Scenario 1** – Create a Denial of Service / Annoyance for the CubeSAT operators
- **Scenario 2** – Modify data being sent by the CubeSAT
- **Scenario 3** – Upload a malicious application to the CubeSAT to kill the radio
CubeSAT Attack Demo Videos
Please download higher resolution PDF of attack tree from https://www.sci-zone.com/cubesat-cybersecurity-challenge
Attack Tree – Scenario 2

Please download higher resolution PDF of attack tree from https://www.sci-zone.com/cubesat-cybersecurity-challenge
Please download higher resolution PDF of attack tree from https://www.sci-zone.com/cubesat-cybersecurity-challenge
Section 4: Mitigations Discussion
Mitigation

- General risk management practices are encouraged
- Safety systems on satellites can be adapted for security
- Standards bodies are increasingly issuing guidance on satellite security (NIST PNT Profile)
- Cybersecurity Principles for Space Systems are documented in both academic literature and national policy (SPD-5)
Section 5: Lessons Learned Discussion
CubeSATs are IoT's in space!

Despite cubesats being small, they are still highly calibrated machines that are sensitive to attack

The types of attacks against cubesats are not significantly different than attacks on other cyber-physical control systems

Traditional health monitors for satellites can be used to evaluate security of the cubesat as well
Section 6: Homework
Hackathon
Virtual Machines will be setup on the sci_Zone QuickSAT cloud environment for testing and exploring at https://www.sci-zone.com/cybersecurity-sandbox

- Probe, explore, push, and "hack" the environment!
- You will need to request access from andrew_santangelo@sci-zone.com

- Feedback from participants is welcome!
- Results will be shared with the AIAA Community