SAND2019-8170D

The Center for Cyber Defenders

Expanding computer security knowledge

A STARCS Mission Campaign Project

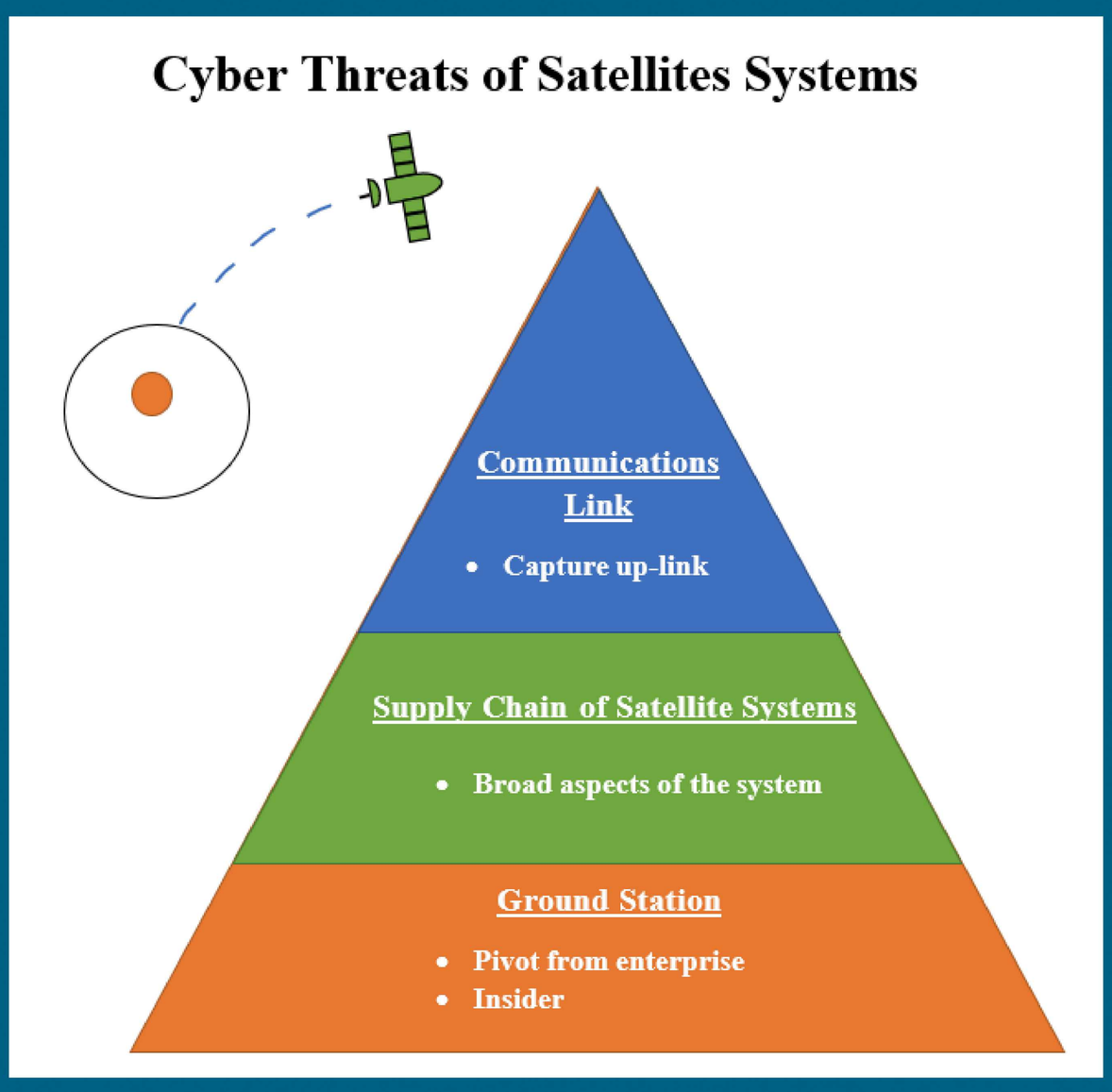
– Towards Cognitive Analytics for Resilient Satellite Systems –

Alexis Cooper, North Carolina Agricultural and Technical State University

Project Mentor: Robert Cole, Org. 5882

Problem Statement:

We need to design, train, test and deploy anomaly detectors in satellite systems. This requires the development of labeled synthetic datasets for training and testing. TCARSS is investigating methods to build (normal, malicious and physical) labeled synthetic datasets for this purpose.



Objectives and Approach:

- Create an experimental satellite system to generate data and explore how it operates based upon the NASA NOS3 simulation package
- Understand how to attack, monitor, and collect data from satellite systems
- Determine methods to generate synthetic data (e.g., Monte Carlo methods)
- Build a more resilient satellite system using machine learning anomaly detectors.

Results:

Attacks

1) Denial of Service (DOS) for Navigation Request
   - Overloading the flight software system with too many navigation telemetry requests sent from ground station
   - Measured that the satellite required a delay of 0.40 seconds to update telemetry from the satellite and report navigation information to the ground station
   - Resulted in the flight software messages displaying 0.00 for the navigational telemetry values.
   - Scripted attacks in Ruby
2) DOS on Camera Experimentation
   - Scripted 'background' process to anonymously kill camera experiments, once initiated
3) Cross Camera and Navigational Mission Impacts
   - Does the frequency of a camera experiment slow down the delivery of navigational telemetry data?
   - Determine how many packets are transmitted and reported to the ground station for a camera experiment
   - Determined that minimal to no cross impact between missions

Impact and Benefits:

- Demonstrated feasibility of scripting attacks against satellite systems.
- Will result in ability to automate dataset collection.
- Leading to the develop and deployment of machine learning analytics to defend against cyber-attacks.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.