STARCS

SAND2020-11230PE

AIRSS: Adaptive Intrusion Response for Space Systems

Project Team: Meghan Galiardi (PI), Jamie Thorpe, Stephen Verzi, Srideep Musuvathy, Eric Vugrin, Matthew Dykstra, McKade Umbenhower

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.

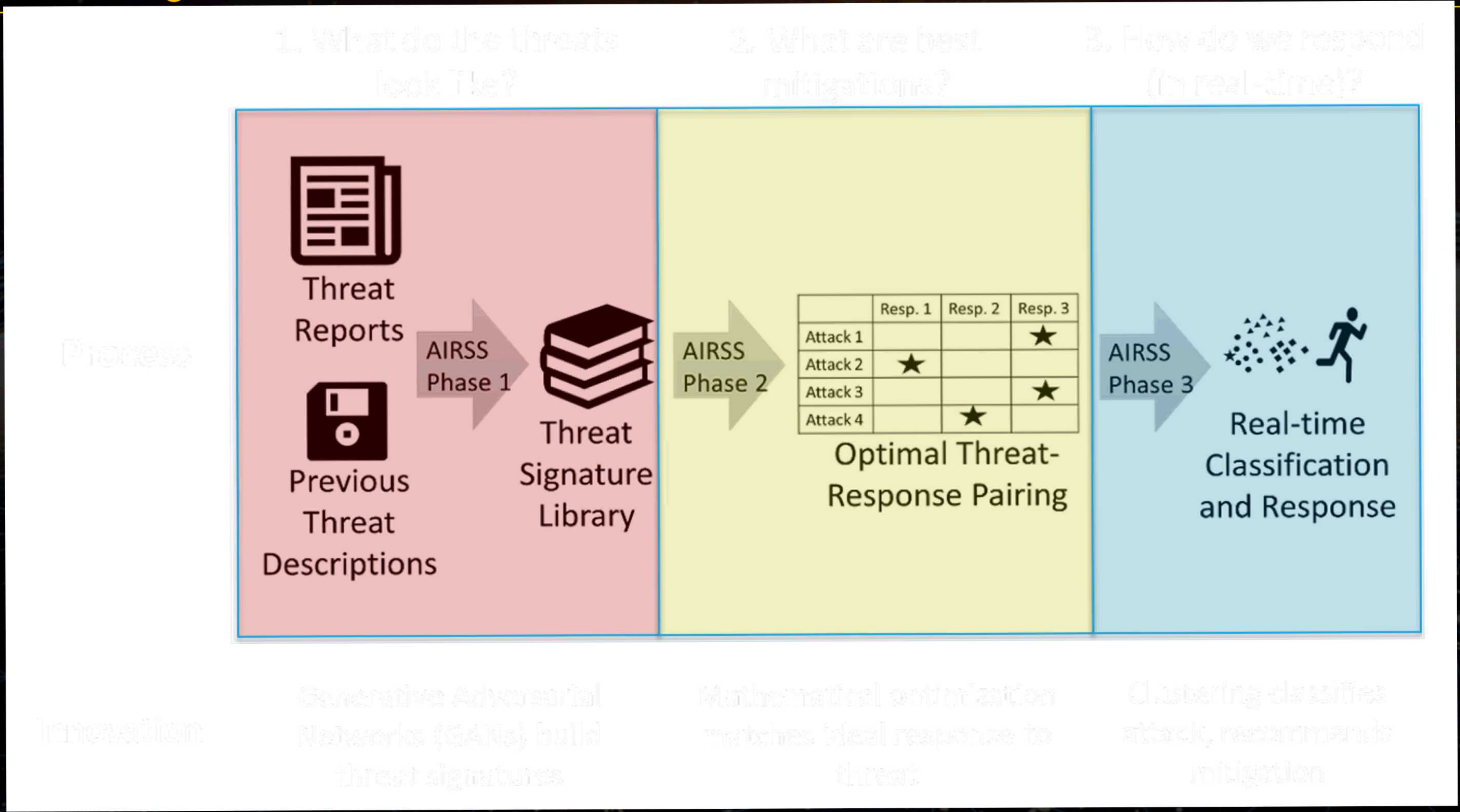
Project Overview

We will develop an onboard response engine to increase the cyber resilience of space systems against cyber attacks.

- The space community recognizes that prevention of all cyber-attacks is an impossibility.
- Cyber security measures need to be complemented with resilience technologies that overcome a spectrum of cyber-physical threats and ensure the survival of mission critical assets.
- Improved cyber resilience requires detection of attacks, recognition of attack types, and rapid identification of effective responses.
- Most of the current cyber resilience research focuses on detection, but only limited efforts aim to use the detection information for improved response.

Technical Approach

The Adaptive Intrusion Response for Space Systems (AIRSS) platform will integrate sensor data to classify cyber threats and recommend proactive countermeasures that defeat them to optimize mission operation through an attack

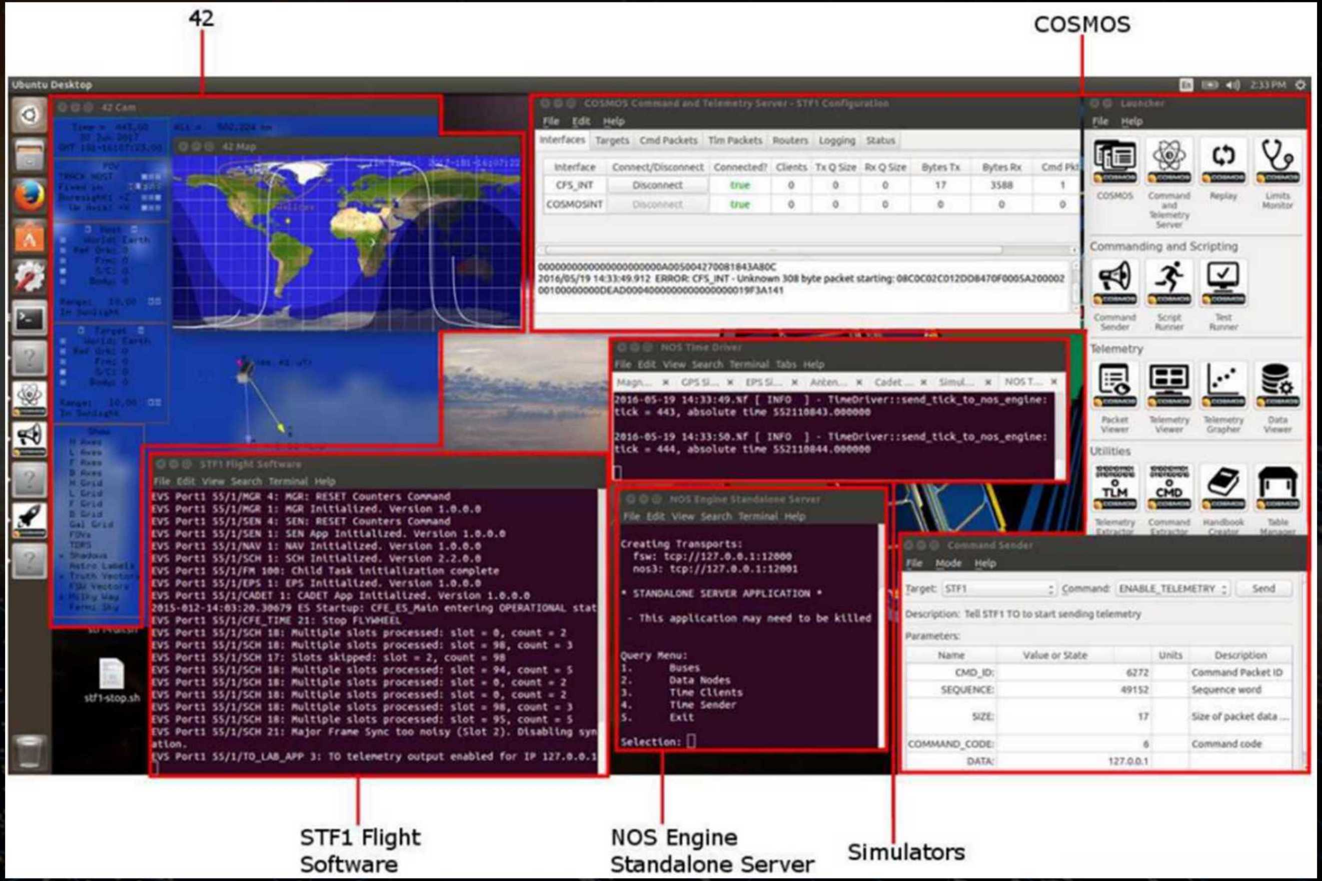

1. What do the threats look like?
2. What are best mitigations?
3. How do we respond (in real-time)?
Process
Threat Reports
Previous Threat Descriptions
AIRSS Phase 1
Threat Signature Library
AIRSS Phase 2
Optimal Threat-Response Pairing
AIRSS Phase 3
Real-time Classification and Response
Innovation
Generative Adversarial Networks (GANs) build threat signatures
Mathematical optimization matches ideal response to threat
Clustering classifies attack, recommends mitigation

	Resp. 1	Resp. 2	Resp. 3
Attack 1			★
Attack 2	★		
Attack 3			★
Attack 4		★	

STARCS

End-to-end Demonstration

- 8 space/cyber SMEs participated in two brainstorming sessions to identify threats of concern and mitigations
    - 21 attacks
    - 13 mitigations
    - 6 measures of system performance
- Developed initial demonstration scenario in NOS3
    - 5 different attack variations on a command table injection attack
- Augmented NOS3 to facilitate better experimentation
    - Added better data collection techniques
    - Added functions/commands to start implementing additional attacks and mitigations



Interface	Connect/Disconnect	Connected?	Clients	Tx Q Size	Rx Q Size	Bytes Tx	Bytes Rx	Cmd Pkt
CFS_INT	Disconnect	true	0	0	0	17	3588	1
COSMOSINT	Disconnect	true	0	0	0	0	0	0

```
000000000000000000000A005004270081843A80C
2016/05/19 14:33:49.912  ERROR: CFS_INT - Unknown 308 byte packet starting: 08C0C02C012DD8470F0005A200002
0010000000DEAD00040000000000000000019F3A141
```

```
2016-05-19 14:33:49.%f [ INFO  ] - TimeDriver::send_tick_to_nos_engine:
tick = 443, absolute time 552110843.000000

2016-05-19 14:33:50.%f [ INFO  ] - TimeDriver::send_tick_to_nos_engine:
tick = 444, absolute time 552110844.000000
```

```
EVS Port1 55/1/MGR 4: MGR: RESET Counters Command
EVS Port1 55/1/MGR 1: MGR Initialized. Version 1.0.0.0
EVS Port1 55/1/SEN 4: SEN: RESET Counters Command
EVS Port1 55/1/SEN 1: SEN App Initialized. Version 1.0.0.0
EVS Port1 55/1/NAV 1: NAV Initialized. Version 1.0.0.0
EVS Port1 55/1/SCH 1: SCH Initialized. Version 2.2.0.0
EVS Port1 55/1/FM 100: Child Task initialization complete
EVS Port1 55/1/EPS 1: EPS Initialized. Version 1.0.0.0
EVS Port1 55/1/CADET 1: CADET App Initialized. Version 1.0.0.0
2015-012-14:03:20.30679 ES Startup: CFE_ES_Main entering OPERATIONAL stat
EVS Port1 55/1/CFE_TIME 21: Stop FLYWHEEL
EVS Port1 55/1/SCH 18: Multiple slots processed: slot = 0, count = 2
EVS Port1 55/1/SCH 18: Multiple slots processed: slot = 98, count = 3
EVS Port1 55/1/SCH 17: Slots skipped: slot = 2, count = 98
EVS Port1 55/1/SCH 18: Multiple slots processed: slot = 94, count = 5
EVS Port1 55/1/SCH 18: Multiple slots processed: slot = 0, count = 2
EVS Port1 55/1/SCH 18: Multiple slots processed: slot = 0, count = 2
EVS Port1 55/1/SCH 18: Multiple slots processed: slot = 98, count = 3
EVS Port1 55/1/SCH 18: Multiple slots processed: slot = 95, count = 5
EVS Port1 55/1/SCH 21: Major Frame Sync too noisy (Slot 2). Disabling syn
ation.
EVS Port1 55/1/TO_LAB_APP 3: TO telemetry output enabled for IP 127.0.0.1
```

```
Creating Transports:
  fsw: tcp://127.0.0.1:12000
  nos3: tcp://127.0.0.1:12001

* STANDALONE SERVER APPLICATION *

 - This application may need to be killed


Query Menu:
1.      Buses
2.      Data Nodes
3.      Time Clients
4.      Time Sender
5.      Exit

Selection:
```

Target: STF1 Command: ENABLE_TELEMETRY

Description: Tell STF1 TO to start sending telemetry

Parameters:

Name	Value or State		Units	Description
CMD_ID:	6272			Command Packet ID
SEQUENCE:	49152			Sequence word
SIZE:	17			Size of packet data ...
COMMAND_CODE:	6			Command code
DATA:	127.0.0.1			

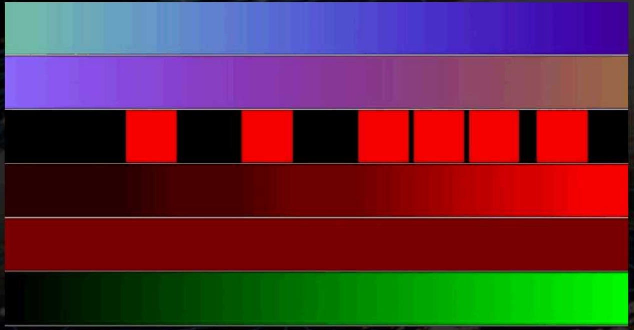
Thank you!

Questions?

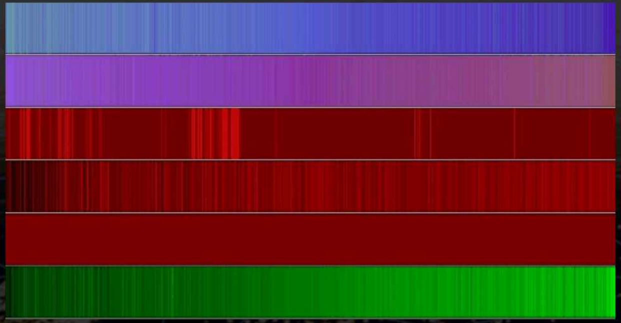
Backups

Threat Signature Generation Algorithms

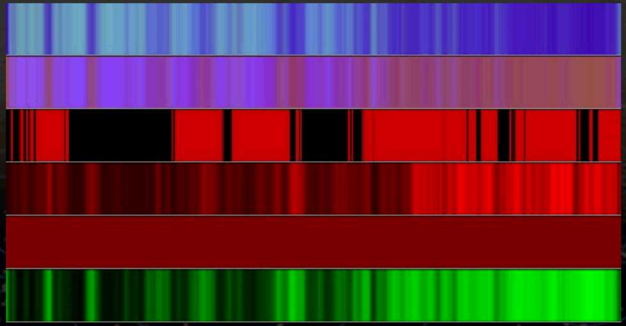
- Developed and tested three algorithm classes: GANs, VAEs, TICC
- Created and implemented evaluation technique to quantifying quality of generated data
- Created custom data visualization to aid in evaluation of generated data
- Tested on NOS3 data and mapped out strengths & weaknesses of each algorithm (see backup slides)
- Significant advances: extending existing algorithms to address temporal complexities in data and adding generative components, and quantifying quality of generated data



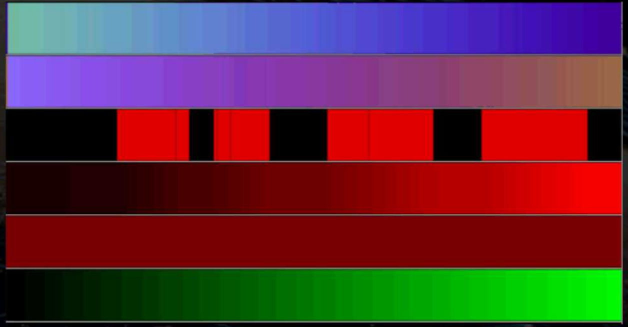
Real data



GAN generated data



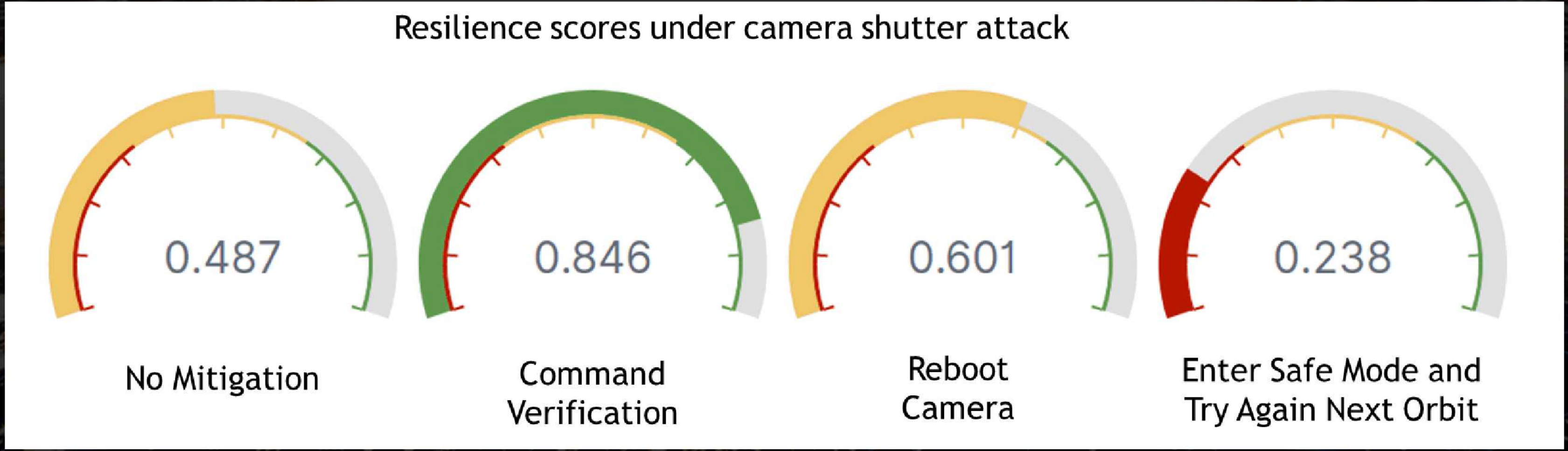
VAE generated data



TICC generated data

Optimal Threat Response Pairing

- Integrated Sandia’s REsilience VeRification UNit (RevRun) with NOS3
- Extended RevRun to work with data from NOS3 by implementing additional preprocessing and metric functions
- Tested on a single attack example from NOS3


Resilience scores under camera shutter attack
No Mitigation
Command Verification
Reboot Camera
Enter Safe Mode and Try Again Next Orbit