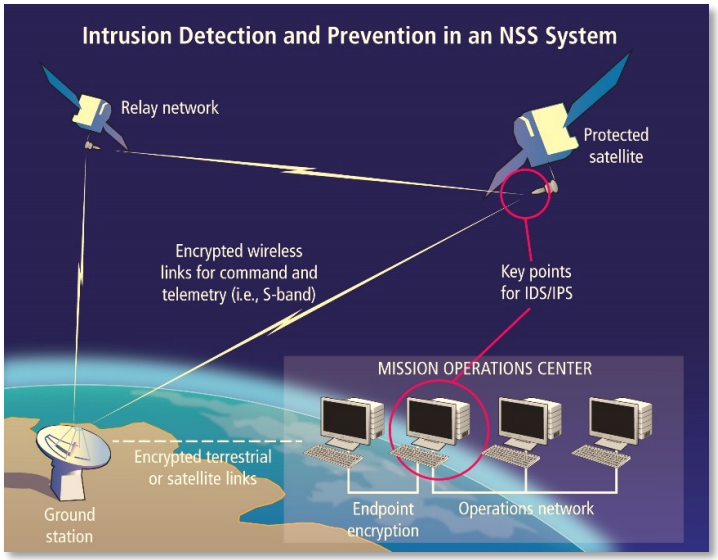
Space Vehicle Onboard Cyber Defense using AI/ML

Nicholas Cohen

GSAW 2022

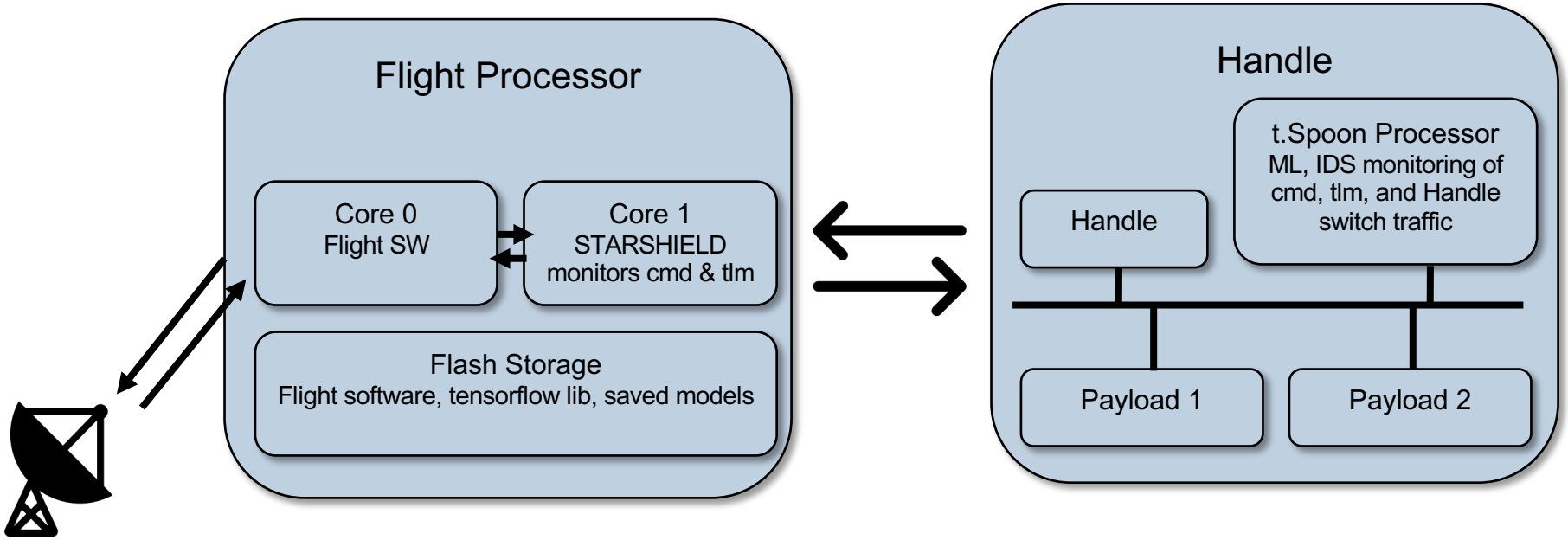
Intrusion Detection in Space Systems

- Limited characterizations of the threats, vulnerabilities and mitigations for the space segment and the space to ground interfaces
- Continuous monitoring for intrusions can alert operators to attacks in real-time
- Extensive research and experience using IDSs and IPSs in ground networks, but require adaptation to work with space systems and specialized protocols



Slingshot Smallsat Platform

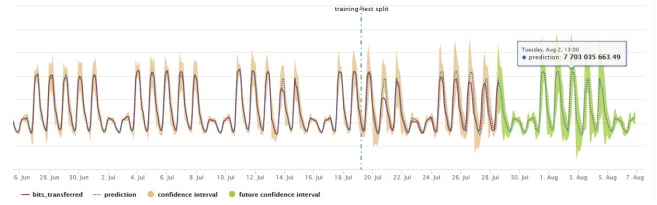
- Aerospace is building a demonstration cyber-hardened space platform
- Two components:
  - *Flight processor*
  - *t.spoon processor (high-performance Zynq Ultrascale+ payload processor)*

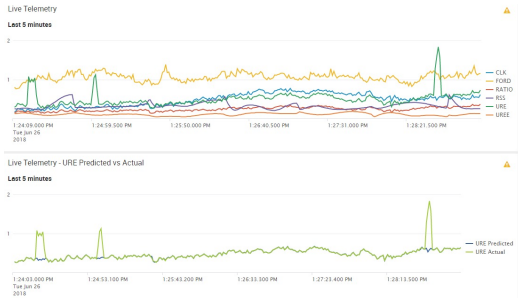


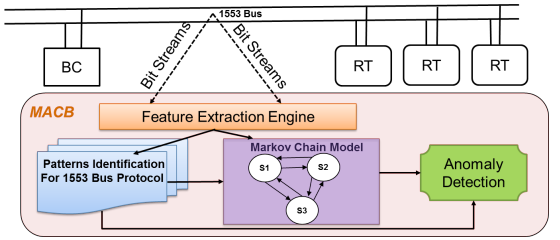
Applications of Machine Learning for Cyber Anomaly Detection

- Command anomaly prediction
  - *Learn normal operational command sequences and generate alarms on unusual commands or sequences*
- Telemetry anomaly prediction
  - *Estimate complex relationships among variables (e.g., telemetry values)*
- Vehicle bus traffic pattern prediction
  - *Detect unusual traffic patterns on the bus*
- System state anomaly detection

- Aerospace is developing prototypes to guide applying machine learning to space data in each of these areas

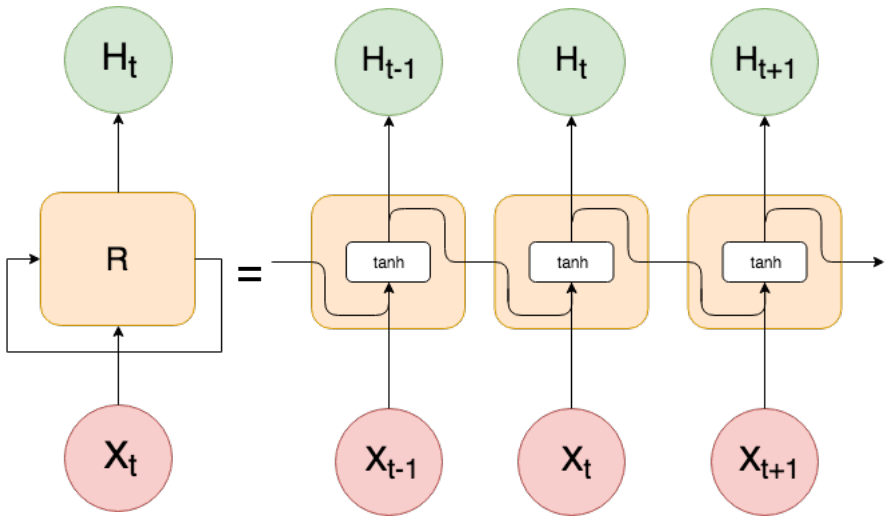






LSTMs

Recurrent Neural Networks [1],[2]

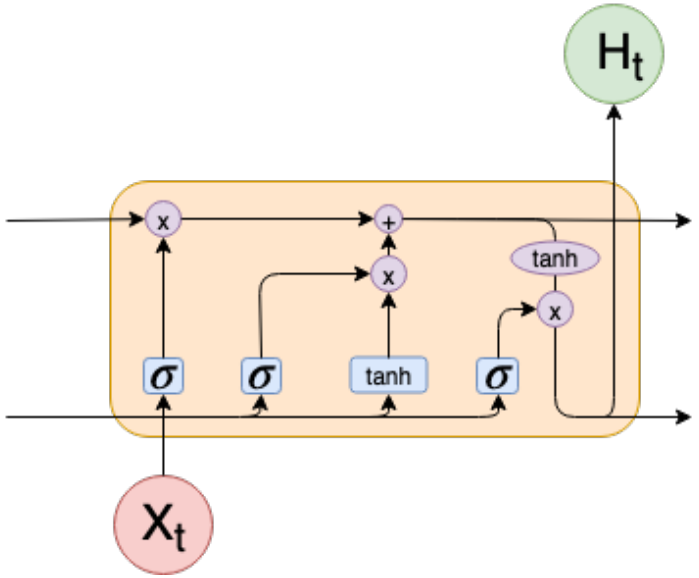


RNNs

- A form of temporally aware neural networks
- Information passed in loops through the network
- Usually consist of single $\tanh$ operation
- Trouble with long term dependencies

LSTMs – Long Short Term Memory

- Address long term dependency issue of vanilla RNNs
- Four neural network layers/gates
  - Forget
  - Input
  - Candidate
  - Output



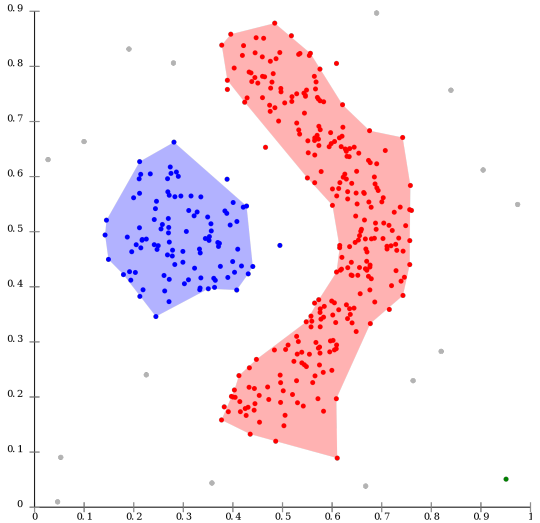
Choice of LSTMs mitigates losing long term patterns

Density Based Clustering

Non-Parametric clustering with outliers [3][4]

DBSCAN - Density-based spatial clustering of applications with noise- Ester, Kriegel, Sander, Xu

- Density Based
- Non-parametric
- Dense regions become clusters
- Points in sparse regions are outliers



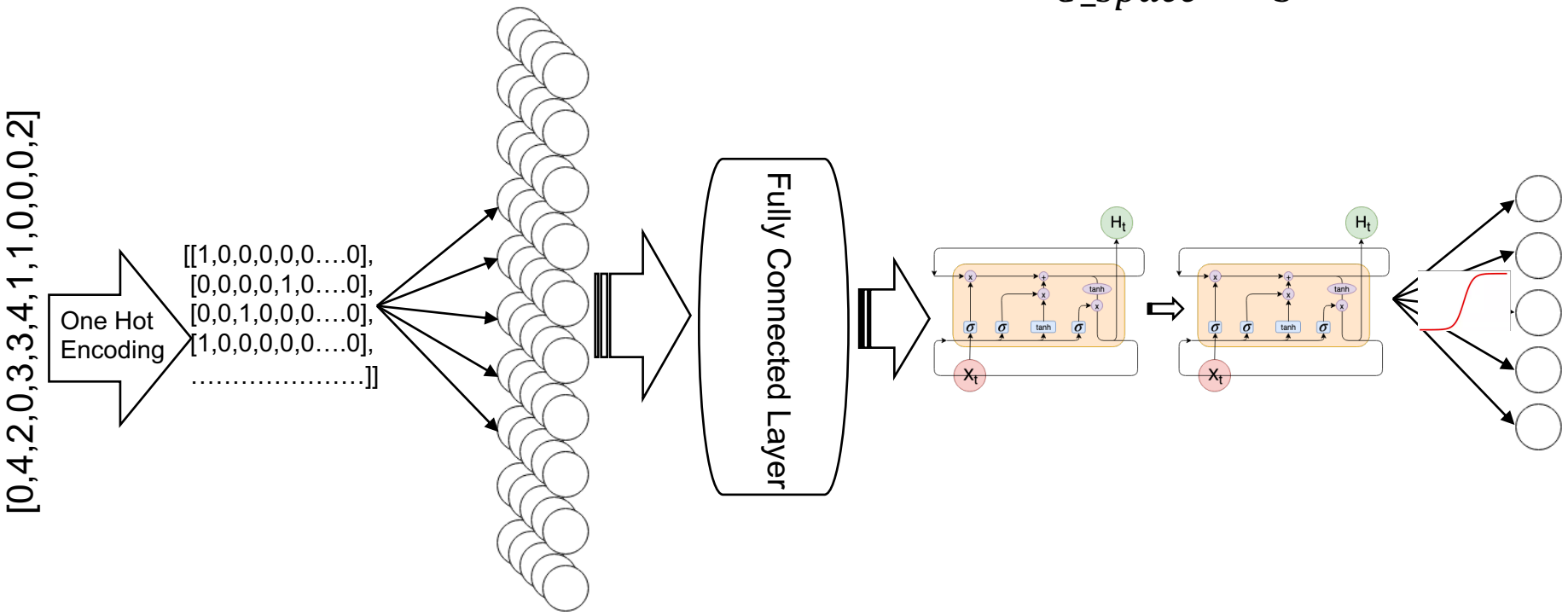
The DBSCAN algorithm can be abstracted into the following steps:[]

1. Find the points in the ε (eps) neighborhood of every point, and identify the core points with more than minPts neighbors.
2. Find the connected components of *core* points on the neighbor graph, ignoring all non-core points.
3. Assign each non-core point to a nearby cluster if the cluster is an ε (eps) neighbor, otherwise assign as outlier.

Command Anomaly Detection

Example Model Architecture

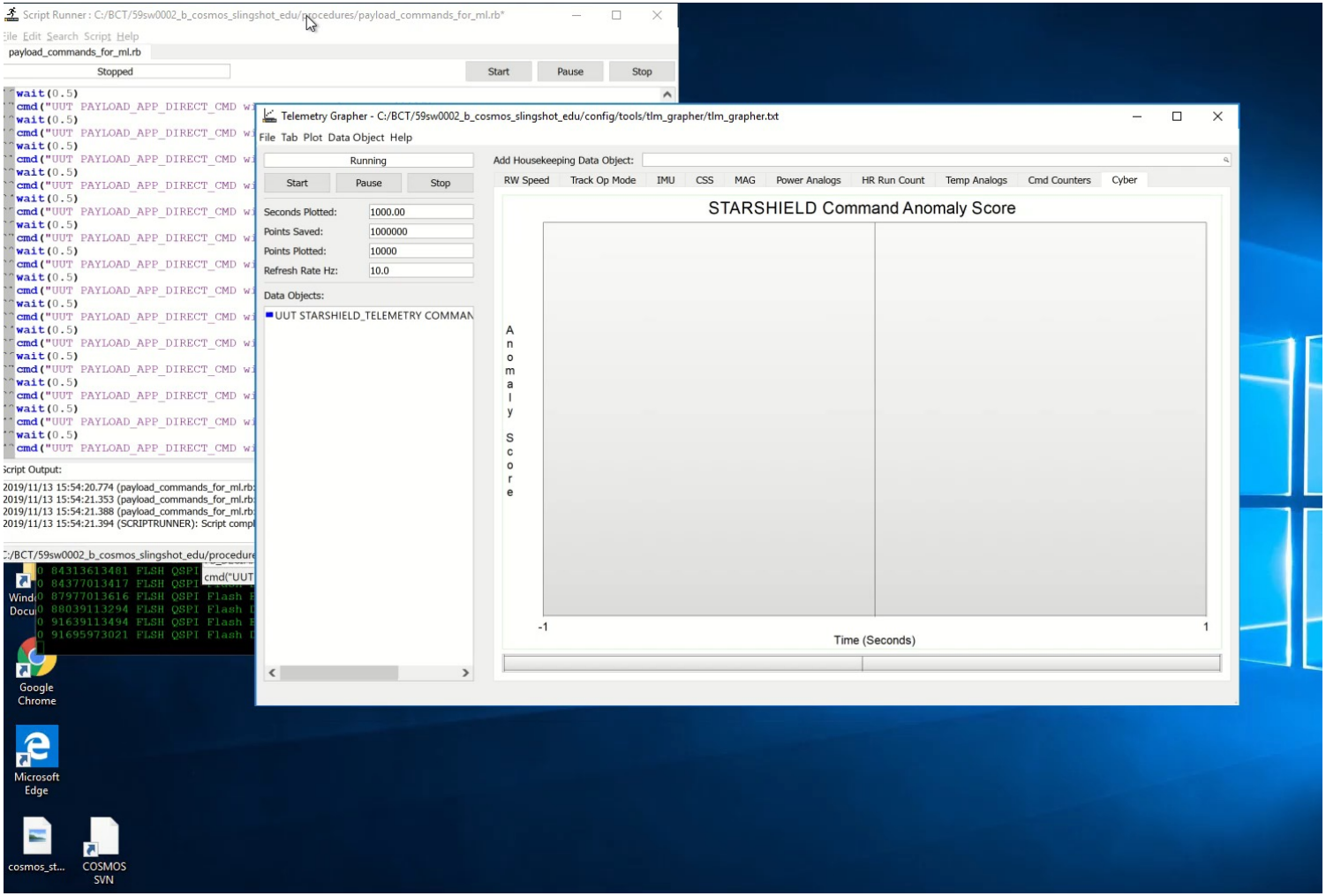
$$P = 10$$
$$C\_space = 5$$



Name	Input	Dense	LSTM 1	LSTM 2	Output
Dimensions	$1\ x\ P\ xC_{space}$	128	32	32	C_{space}
Activation	None	Relu	tanh	tanh	softmax

STARSHIELD

Demonstration



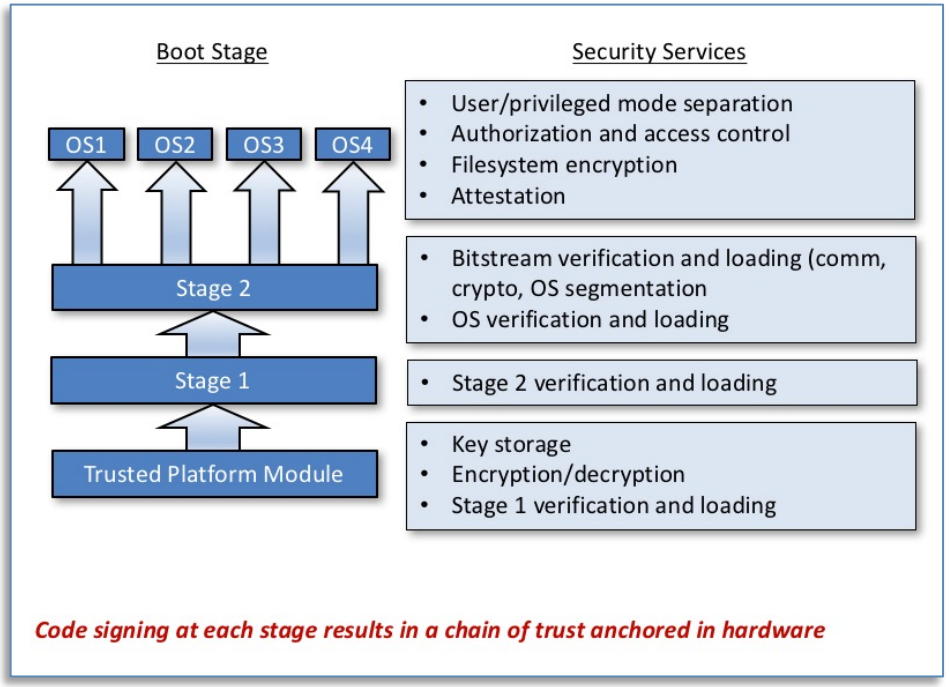
Spacecraft Security

Mission and Objectives

- Shape the future of spacecraft security by solving difficult, unanswered problems affecting the enterprise:
  - *How do we enable lightweight cryptography on cubesats?*
  - *What are the elements of a fully secure satellite security implementation?*
  - *Which security elements are the most important?*
  - *What can be done for existing satellite architectures (add-on security)?*
  - *What emerging technologies are most promising to enhance security & are resilient to future adversarial tactics?*
- Government needs help:
  - *In-lab research which can be extracted to recommendations/ requirements/ evaluations for programs of record*
  - *Development of prototypes which demonstrate emerging technologies*
  - *Platform for training and cyber exercises*
  - *Operational equipment to support security testing*

Secure Boot

- Secure boot for the Zynq Ultrascale+ is accomplished by using the Xilinx encryption boot mechanism, which encrypts all boot or configuration files.
- The Zynq Ultrascale+ is a representative space platform that offers security features that can often be underutilized. Leaving the spacecraft more susceptible to cyber-attacks.
- What AES Secure Boot offers:
  - *Integrity*
    - AES Secure Boot protects the spacecraft from adversaries being able to upload and execute their own flight system software. Without the AES key, you would be unable to run any malicious boot image.
  - *Confidentiality*
    - By having the flight system software encrypted, you protect the flight software and deter any attempt at reverse engineering.



Cyber Hardened Payload Prototype

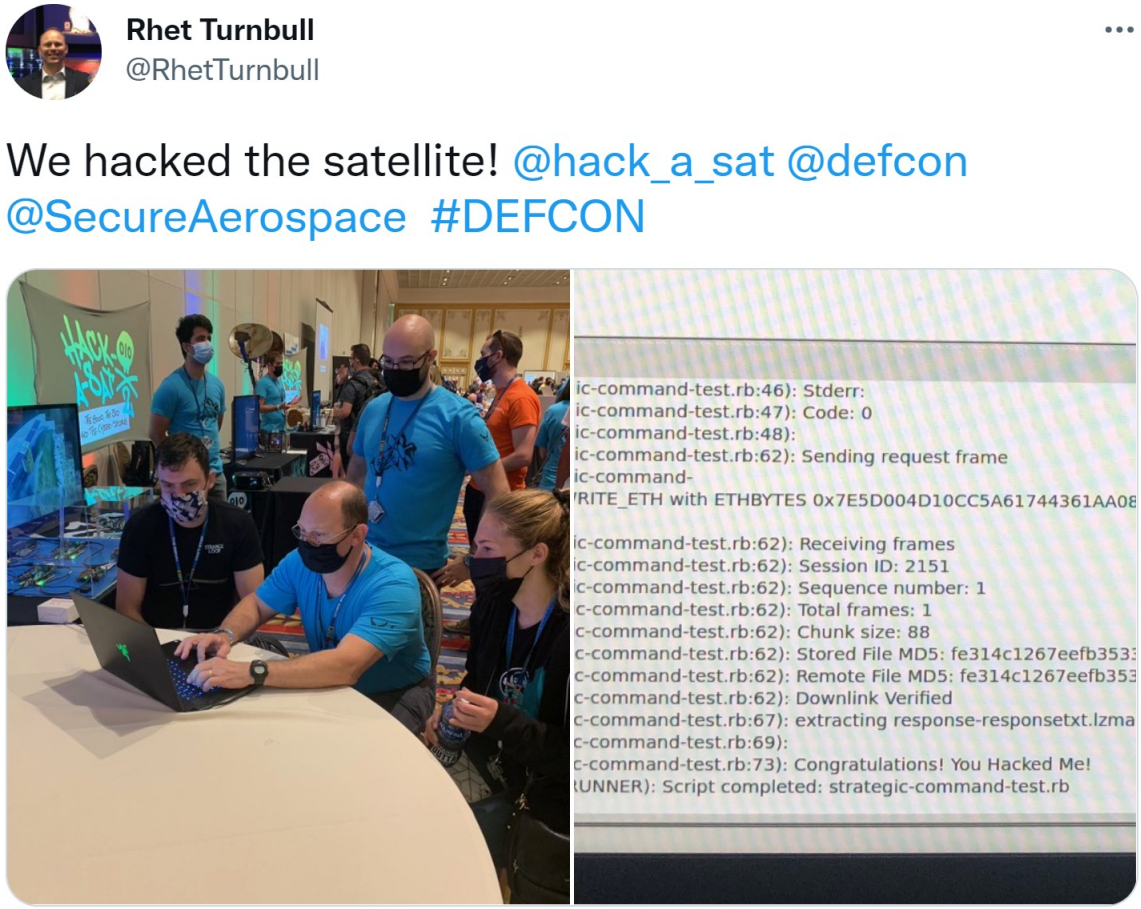
Cyber event collection flying on Slingshot 1

- Current prototype is going to fly on the tSpoon Processor (Zynq FPGA) payload on the Slingshot One mission.
- Built on hardware root-of-trust

- On the payload we have:
  - Cyber event collection and querying based on Elasticsearch
  - Linux sensors monitoring:
    - SELinux Audit log data
    - Integrity Measurement Architecture logs
      - *Every file change and process execution is hashed and logged in our system*
  - *TensorFlow integration to enable ML-based telemetry anomaly detection*

DEF CON Capture-the-Flag

DEF CON Capture-the-Flag



DEF CON Team


HACK-A-SAT 2
010
FEATURED EVENTS AT DEF CON 29
The Antenny Board Design and Fabrication Saga: Sweat and Tears Along the Supply Chain
AUG 6 /// virtual
Hack-A-Sat 2: The Good, The Bad and the Cyber-Secure
AUG 6 /// virtual
Hack-A-Sat 2 Satellite Platform
AUG 6 & 7 /// virtual and in person
Nyansat v2/Antenny
AUG 6 & 7 /// virtual and in person
Understanding Space in the Cyber Domain
*2 sessions: AUG 6 & 7 /// virtual only
aerospacevillage.org/events/upcoming-events/def-con-29
HACKASAT.COM


Thank you!
Questions?