Model-based Approaches for Cyber Risk Assessment of Space Missions

Dr. Arun Viswanathan
aviswant@jpl.nasa.gov
Cyber Defense Engineering and Research Group

Jet Propulsion Laboratory
California Institute of Technology

About Me

M.S., Ph.D. in Computer Science (Cybersecurity)

Dec 2015
University of Southern California
Advisor: Dr. Clifford Neuman

Manager, Cyber Defense Engineering and Research Group @ JPL

Apr 2015 - *present*

- Lead technology development projects and cyber research

Research interests

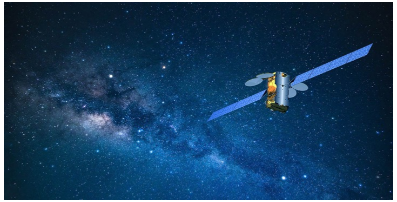
- “AI for Cyber defense”
  - Model-based Reasoning and Analysis
  - Detection, diagnosis and response
  - AI/ML techniques for cybersecurity
- “Cyber defense of AI”
  - Security of Autonomous and Intelligent Systems

State of Cybersecurity

Cyber attacks have real impacts to society!

2009: Stuxnet worm infects the Natanz nuclear facility in Iranian targeting centrifuges used for Uranium enrichment.

2021: Hacker tries to poison Florida Water Supply by increasing the concentration of Sodium Hydroxide



2022: Cyberattack against KA-SAT (owned by Viasat) takes down internet connectivity for thousands of people in Ukraine.

2021: Hackers take down colonial pipeline leading to fuel shortages across the US east coast

The Threat Landscape for Space and Autonomous Systems

Attacks on Ground Systems

E.g. April 2005
A rogue program penetrated NASA KSC networks, surreptitiously gathered data from computers in the Vehicle Assembly Building, and removed that data through covert channels

Attacks on Comm. Links

E.g. March 2014
A number of television channels broadcast through Arabsat's network of satellites were jammed by signals coming from Ethiopia.

Attacks on Spacecraft/ Autonomous Capabilities

E.g. June/July 2008
Terra EOS AM-1/Landsat-7
Attempted satellite hijacking, hackers achieved all steps for remote command of satellite

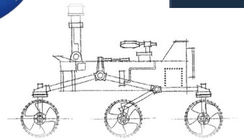
More examples: SPACE Cybersecurity's Final Frontier. London Cyber Security (LCS) June 2015 report.

Cyber Defense Engineering and Research (CDER) Group

15+ members, Diverse Backgrounds

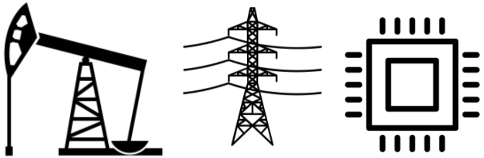
Cyber Defense Engineering for Missions

- Assist missions with cybersecurity across their life cycle phases.
- Tools and expertise deployed across several JPL missions (e.g. Mars missions, Europa mission, Deep Space Network) and have been in operation for 5+ years.



Technology development / Fundamental research in Cyber Security

- JPL funded research
- Non-NASA Reimbursable tasks (Power Grid, Oil and Gas, DoD, NSF, DARPA)
- Research areas: Intelligent Cyber Defense Technologies for Space, Security of Autonomous and/or Intelligent Systems, Human-machine teaming for cybersecurity, Secure System Design, Secure Avionics



"Oil Derrick" by Nikita Kozin, from thenounproject.com
"Transmission Tower" by Arthur Shlain, from thenounproject.com
"Processor" by Creative Stall, from thenounproject.com

Challenges for Space Cyber Security

Why cyber for space systems is hard?

- Culture and Mindset
- Networked, complex and distributed
- Space research is very collaborative
- Mission critical systems
- Legacy systems and components
- Supply chain risks
- Long development times
- High-value Targets

Automating Cyber Risk Assessment Using Model-Based Approaches

Goal

Perform a repeatable cyber-risk assessment that takes into account mission objectives.

Cyber Risk Assessment

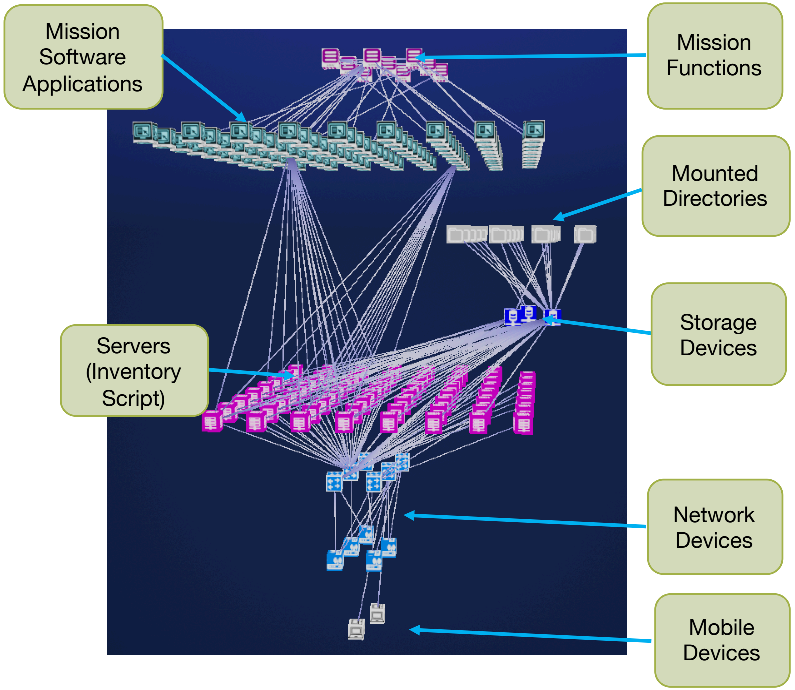
- Purpose is to capture information about the threat environment, vulnerabilities, identify risks, and evaluate controls designed to mitigate damage from an attack or failure
- Two main NIST Documents that guide cyber risk assessment
  - NIST SP 800-30 (Guide for Conducting Risk Assessments)
  - NIST IR 8179 (Criticality Analysis Process Models)
- There will be new requirements for missions to conduct a cyber risk assessment

Past Challenges with Risk Assessments

- Risk assessments are usually table top exercises performed with missing and outdated information
  - Functional Design Documents
  - Bedsheet Diagrams
  - System Data
  - Subsystem SMEs

- The time needed to perform a risk assessment is often exorbitant
  - Previous cyber risk assessment for a mission would take around 4-6 months

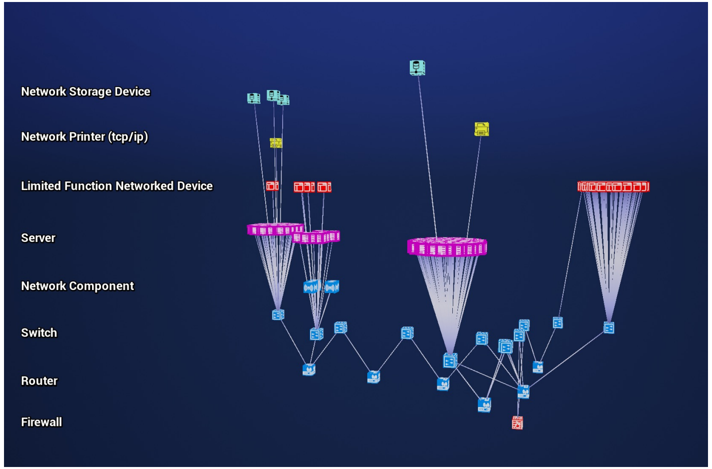
Cyber Analysis and Visualization Environment



- JPL-developed, extensible, software framework to be used by cyber analysts.
- Multi-layered cyber-physical system model
  - Hardware, software, files, processes, network connections, vulnerabilities , cost, risk
- Model-based reasoning
  - Determine consequences of adversarial activities to mission objectives
  - Report cyber-physical inventory to the mission
  - Track possible adversary entry/paths/goals given known weaknesses in our mission environment (i.e. CVEs, node centrality, proximity to the internet)
- Currently modeling missions in flight and development

Getting Data into CAVE

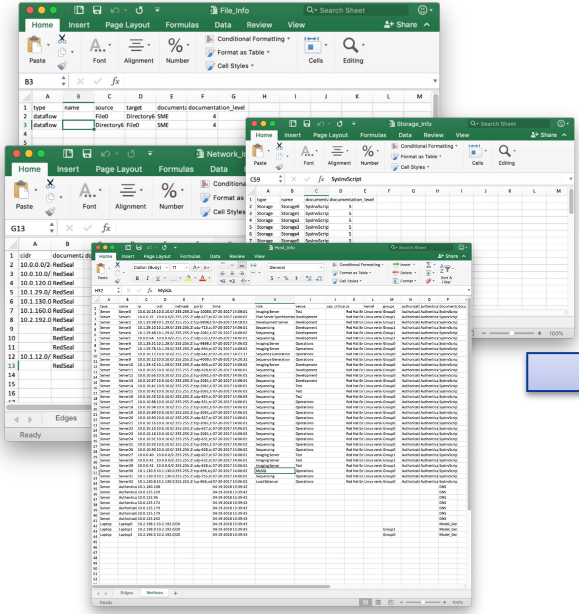
- **Host Data**
  - Custom Scripts
    - RedHat 5 and RedHat 7
    - Solaris 8,9,10
  - Splunk Forwarder (Data Collector)
  - Nmap (Network Mapper)
- **Vulnerability Data**
  - Nessus (Vulnerability Scanner)
  - Vulnerability DB (MITRE)
- **Network Information**
  - RedSeal (Network Mapper)
- **Mission**
  - Workflows
  - Mission Software
  - Criticality

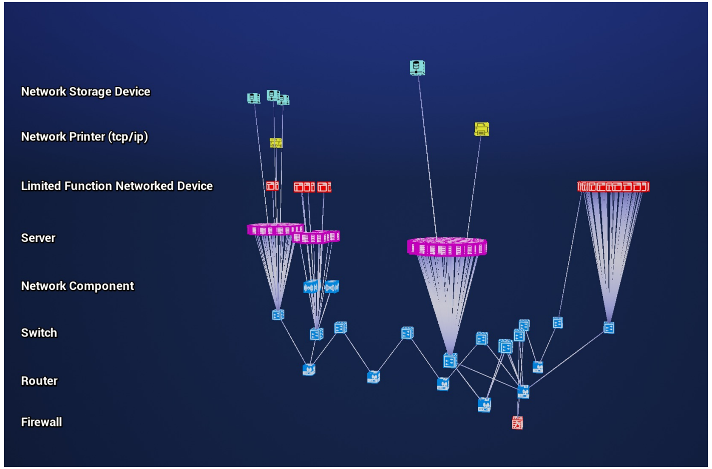


Common input format for all data

Interactive visualization of mission data

Getting Data into CAVE



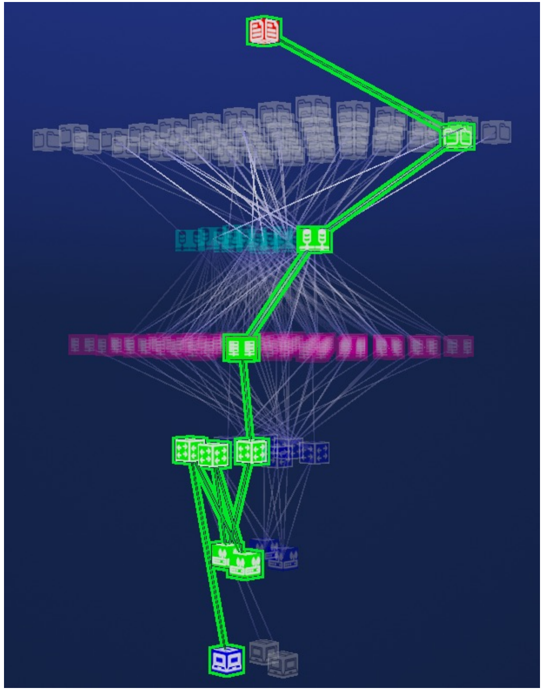


Common input Format for all data

Interactive visualization of mission data

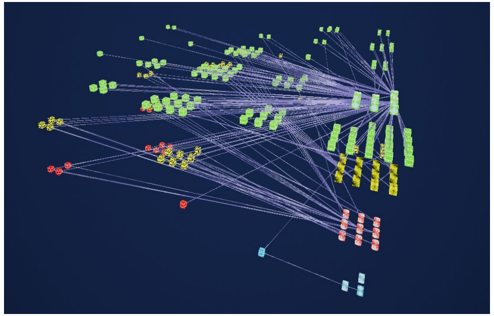
Example Model-based Reasoning in CAVE

- On which ports can two servers communicate?
- What mounted directories can a server read?
- Are there any critical vulnerabilities on servers that can run a mission critical application?
- Which systems have a vulnerability with a downloadable exploit?
- Can an adversary access a critical mission resource from the internet?

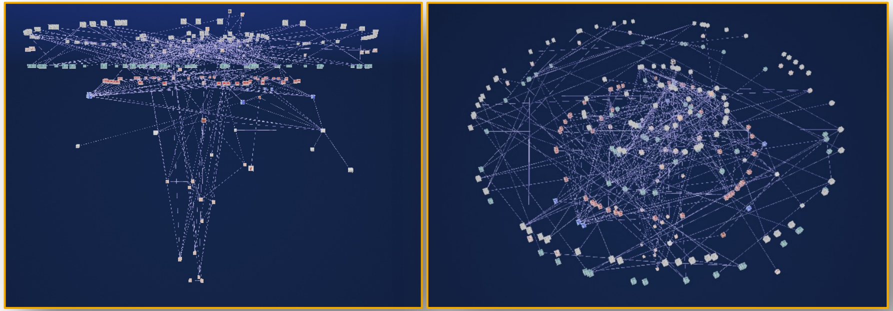


User-Defined Layouts

- User can define the placement of objects from the model using
  - object attributes
  - results of an analysis
  - graph properties



Grouping Nodes Together

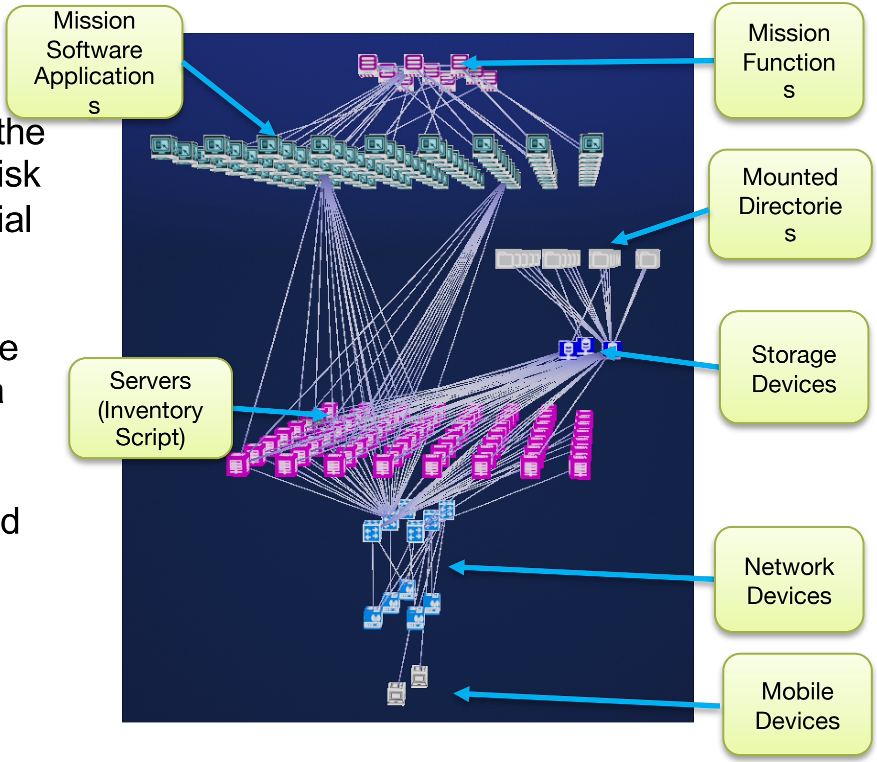


“Hops to Internet” Layout

“Betweenness” Layout

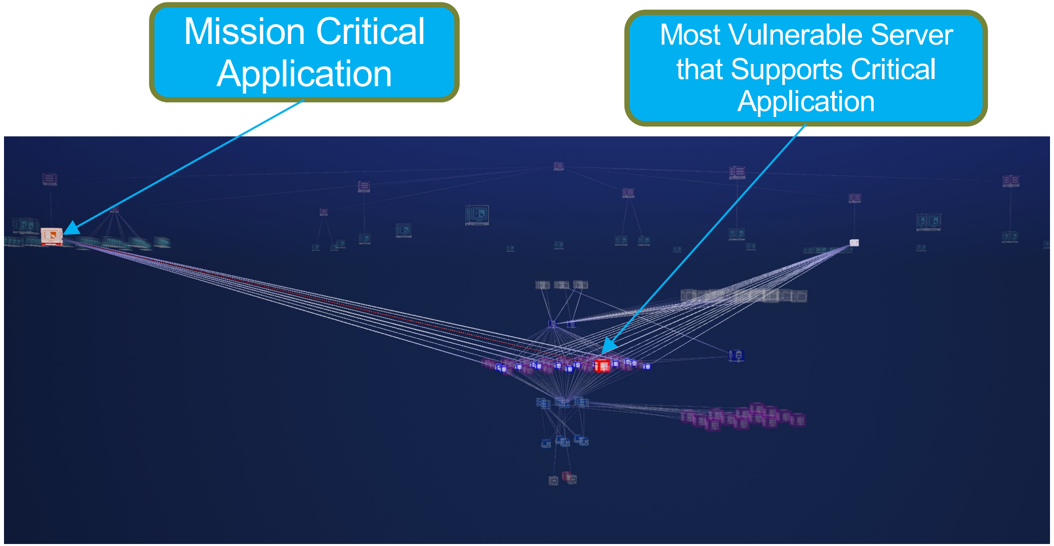
CAVE Use Case for a Mission Project Protection Plan (PPP)

- As part of the Mission's PPP, the mission conducted a Cyber Risk Assessment to identify potential mitigations
- Analysis was conducted by the mission to identify critical data and software products
- Threat analysis was conducted by the mission cybersecurity team



CAVE Model Analytics for PPP

- Find all paths on known vulnerable ports to servers that have access to the command dictionary
- Find all servers with vulnerabilities with a downloadable exploit that compromise data integrity
- **Find all servers with critical vulnerabilities that have exploits available and run mission critical software**



Summary

- Models consolidate distributed, often siloed “tribal knowledge” into a structured representation, amenable to automation.
- Model-based reasoning dramatically reduces the time for identification of security weaknesses from months to minutes, leading to exponentially faster remediations.
- Model-based risk assessments are scalable, repeatable and accurate.

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov