The New Space Race: Cyber Security for Space Missions
Arun Viswanathan, Jeremy Pecharich
Cyber Defense Engineering and Research Group
11 Oct 2016
Agenda

• Threats against space systems
• Cyber security challenges @ JPL
• Cyber defense engineering and research @ JPL
• Projects
  – Cyber Defense Lab
  – Sensor Mesh
  – Botnet Detection
  – Cyber Asset Visualization Environment
• Near-term and Long-term Objectives
The Threat Landscape
JPL builds cool stuff!
Threats to Space Systems

“The single largest vulnerability of space systems today is cyber.”

Mark Maybury, chief technology officer at MITRE Corp. and former Air Force chief scientist

https://www.aiaa.org/SecondaryTwoColumn.aspx?id=21097
Past Incidents against Space Systems

- **January, 2016** – GSFC, GRC, and AFRC. Drone data and command authority hack

- **September, 2014** – National Oceanic and Atmospheric Administration (NOAA) – Chinese hackers breached computer networks to distort operational data coming from U.S. satellites

- **November, 2011** – Attackers were able to penetrate into JPL’s network and take over some services, impacting missions

- **May, 2011** – Goddard Earth Observation System – a hacker gained access to information contained on servers for the satellite-based Earth observation system

- **June, 2011** – Lockheed Martin was attacked using data obtained from the March RSA attack, unclear what was lost from Lockheed

- **2009** – Johns Hopkins University Applied Physics Laboratory – the lab was removed from all external network connections for a month due to the detection of hidden malware and stolen data

- **2007** – NASA Kennedy Space Center – a rogue program penetrated KSC networks, surreptitiously gathered data from computers in the Vehicle Assembly Building, and removed that data through covert channels
The State of Cyber Security: New Malware

Average of ~11 Million New Malware Samples Per Month

State of Cyber Security: Zero Days
Symantec Report: A new zero-day vulnerability every week in 2015

2015 Zero-day Not-So-Fun Facts

- 7 new Industrial Control Systems (ICS) vulnerabilities targeting various manufacturers and devices.
- 11 new zero-days used to exploit open source.
- Average time of exposure for top 5 vulnerabilities in 2015: 7 days
High-level Goals

• **Resilience**
  – The ability to sustain the functions necessary for success in spite of hostile actions or adverse conditions.
  – The ability to make well-informed decisions to sustain mission objectives.

• **Situational understanding**
  – What has happened?
  – Why did it happen?
  – What should I do?
Cyber Security Challenges @ JPL
Unique Cyber Security Challenges @ JPL

- Mission-critical Systems
- Legacy Systems
- Cyber-physical Systems
- Heterogeneous Cyber Systems
- Many collaborators, different collaboration profiles
- Sensitive Operational Environments (low tolerance for uncertainty)
- (Very) Remote High Value Assets
The Problem

• Current COTS products are not deployable in mission environments
  – Imprecise measures of capability, e.g., poor metrics
  – Not built with mission requirements, e.g., adaptability to mission phasing, dial-up/down of resources
  – Poor knowledge and characterization of performance
    • No concept of failure profiles in evolving environments (threat and infrastructure)
    • No science behind the study of errors, e.g., when do errors occur and how can we compensate for them?
  – Many black boxes with no understanding of when and how performance changes cascade to affect down-stream decision-making processes
  – Many claims with little evidentiary support (independent validation)

A severe lack of underlying (scientific) principles to support the effective deployment of defensive technology in mission critical environments.
Cyber Defense Engineering and Research @ JPL
CDER Group

- Dr. Kymie Tan (PI)
- Bryan Johnson (Group Supervisor)
- CS / Math Ph.Ds
- System Administrators
- System/Embedded Programmers
- Software Engineers
- Visualization Engineers
- Hardware Engineers
Cyber Engineering and Applied Research Thrusts

- Survivability – operational resilience through attacks
- Automated detection, diagnosis and remediation
- Design and deployment of anomaly detectors
- APTs and supply chain attack detection
- Modeling for cyber situational awareness
- Design of security metrics
- Rigorous evaluation of cyber defenses in mission-critical environments
- Threat and vulnerability assessments
Non-Nasa Projects

1. **Power Grid**
   - Department of Energy funded Smart Grid Regional Demonstration Program (SGRDP)
   - To develop cyber defensive technologies aimed at protecting the national energy infrastructure

2. **Petrochemical Industry**
   - Protection of the Oil and Gas critical infrastructure against cyber incursions
   - Multi-phased project aimed at infusing resilience into the operational infrastructure

3. **Fort Meade**
   - Precision enhanced calibration of cyber attack sensors
   - Performance evaluation of insider threat sensors
   - Model-based support for rule management of situational awareness engines
Overview of Projects
JPL Cyber Defense Lab

A Secure Test Environment

- Isolatable environment
- Secure USB to transfer data/reports
- WiFi isolation
- Isolatable environment

Rapidly Deploying Cyber Experiments

- Repeatable configuration script
- Configuration created
- GUI to develop/edit configuration scripts
The Sensor Mesh
Big Data Processing and Analytics

Objective: Enhance mission cyber situational awareness

- Decision Making & Response
- Mission-centric Cyber SA
- Data Analytics
- Data Storage / Indexing

- Anomaly detection
- Signature/pattern detection
- Diagnosis of alerts
- Diagnosis of system state
- Correlation and summarization
- False positive reduction
Project:
Cyber Analysis Visualization Environment
Attacks claim hijacking drone almost crashing it into the Pacific

**Context:** Global Hawk Drone Hack (2016)

**Step 1:** Gain foothold on a NASA server.

**Step 2:** Move laterally by compromising SSH passwords.

**Step 3:** Use compromised machine to sniff passwords / gather details of NASA programs.

**Step 0:** Purchase vulnerability.

**Step 4:** Use sniffed admin password to gain access to storage device containing flight logs / drone route files.

**Step 5:** Understand system/drone operations using gathered data.

**Step 6:** Conduct MiTM attack to replace pre-planned drone route file.
Cyber Analysis Visualization Environment (CAVE)

- CAVE provides a user-interface to interact with the system-model network graph.
Multilayered System Model (graph-based)
Threat Modeling Using Attack Trees

- Multilevel diagrams representing the steps an adversary needs to take to achieve a goal
  - Consist of a single objective (root node)
  - Several children nodes (intermediate steps)
  - Edge between two nodes, A and B, if B must be executed immediately before A.
  - Entry nodes (leaf nodes), from which an attacker can begin an attack path to the root node

- Typically constructed via a Cyber Subject Matter expert.
- Annotate the attack tree to link nodes of the attack tree with nodes in the system model
Attack Tree Example

CNA - Computer Network Attack
Attack Tree Example

- Compromise Spacecraft
  - Compromise Spacecraft Command File
    - Send Command File to Spacecraft
      - Gain Proximal Toehold on Network
        - Install Malware at Local Internet Café
          - Name: Internal Laptop
        - CNA Server that Allows Remote Sign-On
          - CNA External Facing Server
            - Type: Server Zone: Unprotected
        - CNA Firewall
          - Type: Firewall
        - CNA Proximal Server
          - Type: Server Subnet: 192.168.24.0/24
            - Type: Storage Name: Command Database
    - Pivot to Server with Database Access
      - Replace Command File
        - Type: File Name: Command File

DEMO: Impact Assessment with CAVE
Contributions

- Hybrid methodology for cyber risk assessment based on attack tree threat models.
- Simple, pragmatic approach to annotating attack trees.
- Algorithm to execute annotated attack trees on a multi-layered model.
- Visual perspective to better enable visualization of a multi-layered network.
Project:
Botnet Detection Using Machine Learning
What is a botnet?

*Interconnected network of malware infected computers controlled by cybercriminals.*
Network-based Botnet Detection Task

Detect malicious inbound / outbound communications (and identify bot hosts if possible)
Our Goal

Build robust and dependable anomaly detectors, deployable in our mission-critical environments.

• Reliable characterization of anomalies and attacks.
• Reliable characterization of operational factors which influence anomaly detection.
• Reliable characterization of algorithms.
• Robust evaluation methodologies.
Challenges for Anomaly Detection

Lots of research, but not much operational deployment

- Accurate baselining of nominal system behavior
  - System behavior evolves over time, requires continuous re-training of models.
- Accurate characterization of anomalies and attacks
  - Anomalies often manifest differently based on system context
- Interpretation/explanation anomaly detection alerts
  - Explain why something was detected? Or not?
- Impact of environmental/operational factors
  - Changes in environment can cause attack signal to manifest differently.
- Adversarial evasion (hiding within normal)
  - Adversaries can make attacks hide within legitimate traffic.
- Impact of adversary-induced noise (changing the normal)
  - For example, conditioning of network traffic to maliciously train anomaly detectors
- Detection of anomaly vs. an attack
  - Not all anomalies are attacks
Preliminary results from our first subtask

Explore the impact of environmental noise (background network traffic) on botnet signal, and thereby on botnet detection.

**Our Hypothesis:** Attack signal (as captured by selected features) is not necessarily stable under all environmental conditions.

**Key Results**
1. Not all “features” are resilient to noise.
2. Operational noise has an impact on feature selection, and on detection performance.
Near-term and Long-term Objectives
Lots of opportunities

• Anomaly Detection
  – Robust, dependable botnet detection algorithms deployed in operation
  – Principled approaches to designing anomaly detectors for cyber environments
  – Anomaly detection over different types of data

• Cyber Situational Awareness
  – Application of machine learning methods to make sense of data.
  – System modeling and reasoning about security properties

• Automated Detection, Diagnosis and Response
Contact

aviswant@jpl.nasa.gov

pecharic@jpl.nasa.gov