Session 9: Changing Paradigms and Challenges
Tools for Space Systems
Cyber Situational Awareness

Wayne A. Wheeler
The Aerospace Corporation

GSAW 2015, Los Angeles, CA, March 2015
Agenda

- Emerging cyber threats to space systems
- Defense-in-Depth shortfalls
- Tools for Cyber Situational Awareness
- Example Approaches
- Summary
Open Source Reported Space Cyber Incidents

The age of the space cyber attack is here

• **ROSAT**— satellite disabled (1998)
• **Landsat 7**— “cyber interference” (2008)
• **Terra EOS AM-1**— “cyber interference” (2008)
  – ”achieved all steps required to command the satellite”
• **IntelsatONE**— DDoS (distributed denial-of-service) attacks (2011)
Factors Driving Cyber Threats to Space Systems

• Space systems are distributed networks of COTS\textsuperscript{1}, and can share vulnerabilities with any commercial infrastructure
  – Aging ground infrastructure can be less secure than current commercial systems (no remediation for emerging threats)
• “100% closed systems” assumptions for space systems are not realistic, in light of Advanced Persistent Threats
  – APTs - highly resourced and motivated attackers
  – Supply chain, FOSS\textsuperscript{2} or commercial software, applications software, upgrades, links to other systems, and insider threats are potential attack vectors
• Threats development has moved up from “hackers” to organized crime and resourced State actors
  – Computing power amplifies asymmetric power
  – Estimated 82,000 new malware discovered daily in 2013
• Potential adversaries are known to be developing (and are sometimes demonstrating) sophisticated cyber attack capabilities against space systems

\textsuperscript{1} Commercial-of-the-Shelf
\textsuperscript{2} Free-and-open-source software
The Advanced Persistent Threat (APT)

The highly resourced and motivated adversary

• The Cyber Threat is active and evolving
  – *Cyber attacks are ongoing and continuous as a means by which adversaries attempt to exfiltrate information, test system responses and identify exploitable attack surfaces*
  – *Space, ground, and user segments must be resilient to the persistent probing, penetration and exploitation attempts by adversaries throughout the stages of a space system life cycle*

• Space Architectures must be **cyber resilient** to all types of threats
  – *“Known” Cyber Threats*
    • Identified “in the wild” as a known vulnerability
    • Usually similar to previous malware
  – *“Unknown” Cyber Threats*
    • Only identified after exploit
    • Zero-day attacks
Tools for Cyber Situational Awareness and Response

*It isn't that they can't see the solution. It is that they can't see the problem.*

G.K. Chesterton
Cyber Threats Landscape

**Known**
Identified Vulnerabilities

- Available technologies
- Global industry response
- Best-practices
  - Defense-in-Depth
  - Network Segmentation
  - Layer 3 Firewalls
  - Aggressive Patch Management
  - Boundary Enforcement
  - IDPS
  - 7x24 Top-tier Security Ops Center
  - Current Software/Hardware

**Unknown**
Zero Day, APT

- Emerging technologies
- Industry struggling to respond
- Cyber Analytic Tools
  - Layer 7 Firewalls
  - SIEM
  - Virtualization Sandbox
  - Cyber Visualization
  - Auto respond systems
- Ineffective without development and Ops expertise
  - Significant costs for start-up Ops

Zero Day- Cyber exploit not previously seen
APT- Advanced Persistent Threat
DPDS- Intrusion Detection & Prevention
SIEM- Security Information & Event Management
An Arsenal to Counter 21st Century Cyber Threats

• “Defense-in-Depth” security architectures are necessary, but not sufficient
  – Need to assume that attackers can find a way inside (APTs)
• Cyber Situational Awareness is critical
  – Instrument computers and networks to report ongoing state and activity
  – Leverage advanced Cyber Analytics Tools to correlate and interpret vast amounts of available data
  – Ensure operator training and procedures to utilize available tools
• Enforce system state of “stacks” through automated tools
  – Leverage global knowledge base developing mitigations to emerging threats and vulnerabilities (i.e. patch management)
• Implement processes to continually review and enhance cyber security protections to space systems
  – Operating budgets need to allocate resources for continual enhancements
Cyber Analytic Tools for Advanced Threats

- Industry has developed various real-time cyber analytic tools to identify and respond to advanced threats.
- Instrumentation highlights patterns of a cyber attack – subtle changes in state on a number of systems can be correlated to facilitate early discovery of an attack.
- Data-Driven Security: emerging capabilities such as Big Data cyber analytics and cyber visualization may enable automated analysis and response to advanced threats.
Security Information & Event Management (SIEM)
Challenges to Implementing SIEM

• Custom SIEM log interfaces need to be built for legacy/unique systems
• SIEM outputs are only as good as the logs generated and the rules defined for the implementation
• Advanced tools do not negate the need for training and procedures
• SIEM tools need to be paired with incident response systems/procedures (I know we’re under cyber attack- so now what are we supposed to do?)
• SIEM itself can be compromised (e.g. insider attacks)
• Cloud providers may not provide logs needed for in-depth SIEM
“Sandbox Detonation” for Zero-day Attacks

- Inbound Content
- Pre-Filtering Intelligence
- Virtualization Sandbox
- Malicious Code Detonation
- Incident Response
- Alarms
- Visualization
- Reports

Is it Suspicious?

Is it Malicious?
Case Study: Target Data Breach

- Attackers gained access to the Target network via weak security at a Target vendor
- Except for the final data exfiltration, almost the entire attack took place within the Target corporate infrastructure
  - Target computers were turned into agents for the attackers
- Target never realized the attack on their own
  - Complete lack of cyber situational awareness
- Despite having installed advanced security systems, Target missed multiple opportunities to thwart the attack
  - Lack of skills to architect, deploy, and manage advanced cyber analytic tools
- To date, there has been no attribution (charges/arrests)
Summary

- The cyber threat to space systems is real and will continue to evolve with increasing capabilities for potential attackers.
- **Cyber Situational Awareness** is critical for all segments of a space system (space, ground networks, ops centers, user terminals).
  - Required to identify, mitigate, and attribute advanced cyber attacks.
- **Cyber Analytics Tools** can provide significant insight into cyber situational awareness.
  - Instrument the network
  - Implement analytics to support security team
  - Must develop (or contract for) expertise necessary to integrate and operate cyber analytic tools.
- Cyber Analytic solutions are evolving—resources must be provided for an “evergreen” refresh approach to cyber security.
Questions?