AFSC/SW Supply Chain Risk Management
Software Support Center

The Technical On-Site C-SCRM Assessment Drives Improvements

By:
Alexander Wright & Parker Bauer
USAF AFSC/SW

DISTRIBUTION A. Approved for public release: distribution unlimited. 75ABW-2024-0015.
Overview

- Who We Are
- Background
- Assessment Process
- What We Learned
- Improvements Observed
- Summary
WHO WE ARE
Who We Are

★ Parker Bauer
  ★ Computer Scientist/Mechanical Engineer
  ★ Six Sigma Black Belt
  ★ Hill AFB
  ★ Director of USAF Software Technology Support Center
  ★ Co-lead of AFSC/SW SCRM Software Support Center
  ★ Private industry supplier quality auditor

★ Alexander Wright
  ★ Computer scientist and a member of the 309 Software Engineering Group
  ★ Software developer for several air and space systems
  ★ Initiated SCRM effort in 2018
  ★ Peterson SFB
  ★ Co-lead of AFSC/SW SCRM Software Support Center
Who We Are
AFSC Software Directorate

Organizational Facts
- 3 Air Force Groups united under AFSC/SW
- Supporting the warfighter since 1978
- 5,000+ software professionals
- 3 primary and 7 Operating Locations (OLs)
- Proven ability to expand 8% annually
- FY23 annual revenue $1.04B
- Support 22 PEOs
- 100+ active projects
- Robust community, academic, and industry partnerships

Mission and Product Lines
- Develop, deliver, support, and sustain war-winning capabilities
- Embedded Weapon System Systems and Software Development
- Primary Product Lines:
  - Platform Integration
  - Mission Computing
  - Weapons
  - Air Vehicle Systems
  - Sensor Systems
  - Mission Support
  - Pilot Vehicle Interface
  - Business Systems

Primary Locations
- Hill AFB
- Tinker AFB
- Robins AFB
- Space Systems
- T-1A/25 Operating Wing
- NGA Partnering
- LMA Partnering
- ICBM Program Office Support
- Satellite Systems Launch Support
- Ground-Based Training
  - Ogden, UT
  - Oklahoma City, OK
  - Warner Robins, GA
  - Peterson SFB, CO
  - NAS-Pensacola, FL
  - Patrick SFB, FL
  - NAS-JRB Ft Worth, TX
  - Offutt AFB, NE
  - Vandenberg SFB, CA
  - JBSA-Randolph, TX

Strategic Initiatives
- F-16, A-10, and E-3 Weapon System Integrator
- B-21 and E-7 Future Weapon System Integrator
- Open Architecture (i.e., Open Mission Systems)
- PRC2 First C-ATO of Development Toolchain in the AF
- Embedded with OEMs on next generation AF Weapons
- Partnering with AFRCO on DevSecOps Pipelines for Embedded Software
- Prototyped Kubernetes on F-16
- Prototyped in-flight software update for multiple platforms
- Leaders in Open Standards Implementations
- Leading DSOP Team 8 on Critical Embedded Systems
BACKGROUND
Background
DODIG-2018-143

- Inspector General (IG) Report Findings in 2018
- USAF Space Command (now Space Force)
- “Desk audits” are not sufficient to identify SCRM risks
- Technical business risk must be evaluated beyond standard business operations
  - Foreign development centers
  - Fabrication and assembly
  - Software source origin
Background
Enterprise Ground Services (EGS)
Space Systems Command (SSC)

- Tasked to create a common ground system for DoD satellite systems with a focus on security and redundancy
  - Establish multiple geographically-separated data centers
  - Ensure multiple hardware and software providers for fail over
- For data center hardware, selected SCRM approach to assure hardware uncompromised per IG concerns
  - Secure the supply chain through validated vendors
Establish CRADAs with the 4 largest US-based IT hardware integrators to rigorously assess development, manufacturing, and assembly processes to ensure they follow SCRM best practices to reduce risk

- Tour/assess factory floors (assembly, integration, and test facilities)
- Review corporate policies
- Assess supply chain of each part and assess counterfeit testing
- Analyze difference between public and federal sales
Background
Air Force SCRM Effort

- SSC effort wound down in 2019
- Formally re-started in June 2020 in 309 SWEG
- Continued the work performed by EGS
- Refined assessment
  - Added software and cloud elements to assessment
  - Improved assessment process
ASSESSMENT PROCESS
Assessment Process
The Three Pillars of SCRM

DoD Information and Weapon Systems

System Integration

Cyber Physical System

Software

Firmware

Hardware

Defense Industrial Base

Global Supply Chain
Assessment Process
SCRM Big Picture

Pre-acquisition
Intelligence Reports
Business Analytic Reports
Technical Onsite C-SCRM Assessments

Post-acquisition
Traditional Assurance Practices
Assessment Process Scope

- General Organizational Practices
- Hardware-Centric Products
  - Design & Test
  - Integration
  - Platform Firmware
  - Platform Software
- Software-Centric Products
- Cloud-Centric Products
A score is not assigned to each question, instead the assessment process looks for specific observations of policies and practices which are mapped to a SCRM threat level shown below.

RMF Compatibility (DoDi 8510.01)

Level 0: Does Not Meet the Standards of Common Practice or Cyber Needs
Level 1: Consistent with common Practice but not Current Industry Standards
Level 2: Consistent with Standard Practice for Current Industry Standards
Level 3: Best in Class Practice and Targets Future Cyber Threats/Risks
Assessment Process
Supplier Overview

- Observations are rated by risk level and compiled by category. Then risks are documented for SPO customer.

<table>
<thead>
<tr>
<th>Category</th>
<th>L0</th>
<th>L1</th>
<th>L2</th>
<th>L3</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational SCRM Practices</td>
<td></td>
<td></td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Hardware Centric Products</td>
<td></td>
<td></td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Organizational Practices in Acquiring, Integrating and Controlling Materials</td>
<td></td>
<td></td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Organizational Practices for Sourcing, Integrating and Controlling Platform Firmware</td>
<td></td>
<td></td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Design, Integration, and Test of Data Center Platforms</td>
<td></td>
<td></td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Development, Software Assurance, and Cyber Controls of Platform Control Software</td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Software Centric Products</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development, Software Assurance, and Cyber Controls of Application Software</td>
<td></td>
<td></td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Cloud Centric Products</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development, Software Assurance, and Cyber Controls of Cloud Infrastructure</td>
<td></td>
<td></td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

- Identified risk for SPO PPP: If Supplier X signing servers are not separated from the development network, then there is the risk of insider threats being able to pass a malware payload as legitimate.
WHAT WE LEARNED ABOUT C-SCRM THROUGH THIS PROCESS
What We Learned
Some Sub-Tier Suppliers Matter
What We Learned
Firmware & Software Are Relevant

- Most hardware appliances contain millions of lines of code
- Also contain operating systems of their own
What We Learned
Software Stove Piping within Companies

- Firmware
- Embedded Software
- Application Software and Its Versions
- Cloud

Product Portfolio
What We Learned
3rd Party Manufacturers

- Very common in many industries
- Can obscure who builds what and where, and such knowledge is protected by NDAs
- Hardware
  - Original Design Manufacturers
  - Part suppliers
  - Engineering and Manufacturing
  - R&D
- Software/Firmware
  - Third Party coders
  - Testing/patching
What We Learned
Who Makes What

The 5 US IT Hardware Integrators

Hewlett Packard Enterprise

ORACLE

DELL Technologies

CISCO

SUPERMICRO

Who Makes These and Where?

[Images of various hardware integrators]
IMPROVEMENTS OBSERVED
Improvements Observed as a Result of the Technical On-site C-SCRM Assessments

- Established CUI process for managing orders, and manufacturing, assembly, and test
- Software development team started enforcing secure coding standards
- Started using tamper tape on shipped products
- Established separate product SKUs for different SCRM RMF levels
- Started requesting SBOMs from external suppliers and creating for their own software
SUMMARY
Summary

- Technical On-site C-SCRM Assessments play a role in gaining a more complete view of a supplier’s risk
- The USAF/USSF is now more aware of several key aspects of C-SCRM through Technical On-site C-SCRM Assessments
- Private companies we all buy from who have undergone assessments have improved their C-SCRM posture
Contact Us

▶ Alexander Wright
  ➢ Alexander.wright.4@us.af.mil
▶ Parker Bauer
  ➢ parker.bauer@us.af.mil
THANK YOU!