309 SWEG Supply Chain Risk Management
Software Support Center

USAF C-SCRM/SBOM

Parker Bauer
USAF/AFMC/AFSC/309 SWEG
Alexander Wright
USAF/AFMC/AFSC/309 SWEG

DISTRIBUTION A. Approved for public release: distribution unlimited. 75ABW-2023-0024.
Overview

- Background
- On-Site Technical Supplier C-SCRM Assessments
- USAF Software SBOM R&D Efforts
- DoD/NNSA Software Assurance CoP SBOM WG Update
- Q&A
Background
Six (6) Current Operating Locations:
Vandenberg AFB, CA – Peterson AFB, CO – NAS-JRB, TX – Offutt AFB, NE – NAS Pensacola, FL – Patrick AFB, FL

~4,500+ Software Professionals Combined

Specializing in Operational Programs, C4I, Mission Support, Test Program Sets and Training Systems

OC-ALC, Tinker AFB
Oklahoma City, OK
(1300+ Personnel)

OO-ALC, Hill AFB
Ogden, UT
(1900+ Personnel)

WR-ALC, Robins AFB
Warner Robins, GA
(1300+ Personnel)
Background
USAF Software Traditional Role

Acquisition Lifecycle Phases

Develop
Software and Firmware

New Capability Integrated into Weapon Systems

Add Code to Software and Firmware

USAF, USA, USN software

Sustainment Phase

Primes

UNCLASSIFIED
On-Site Technical Supplier C-SCRM Assessments
Background
AFSPC C-SCRM Effort

- DODIG-2018-143
- ‘It’s not enough to trust what suppliers tell us. The DoD must validate what they tell us.’
(Trust but verify.)
Background
AFSPC C-SCRM Effort

- Enterprise Ground Services (EGS)
  - Validate C-SCRM posture of 4 major OEM IT hardware suppliers
    - Cisco, HPe, Dell and Oracle
    - To address IG concerns
    - Via On-site Technical C-SCRM Assessments
  - Assigned Aerospace Corp to develop C-SCRM assessment framework (based on NIST 800-161 (RMF))
  - Engaged USAF 309 Software Engineering Group software expertise
On-Site Technical Supplier C-SCRM Assessments
When?

Prior to MS B

Intelligence Reports

Business Analytic Reports

Technical Field C-SCRM Assessments

After MS B

Program Maturity

Traditional Assurance Practices

Pre-Procurement

Post-Procurement
On-Site Technical Supplier C-SCRM Assessments
Which Suppliers?
On-Site Technical Supplier C-SCRM Assessments

Why?

- IG report – “validate”
- Limited view when not intrusive
  - Discovered a 3rd party manufacturing significant internet hardware for a top tier industry supplier that was not discoverable on a commercial supply chain search
  - Observe dedicated DoD or USG development and integration facilities to understand cyber posture
  - Also allows for follow-up for improvement
- Private sector companies perform intrusive audits for multiple purposes – financial, quality, etc. Do not rely exclusively on desk audits.
On-Site Technical Supplier C-SCRM Assessments
What is Assessed?

- DoD Information and Weapon Systems
- System Integration
- Cyber Physical System
- Software
- Firmware
- Hardware
- Defense Industrial Base
- Global Supply Chain
On-Site Technical Supplier C-SCRM Assessments
What is Assessed?

- General Organizational Practices
- Hardware Centric Products
  - Design & Test
  - Integration
  - Platform Firmware
  - Platform Software
- Software Centric Products
- Cloud Centric Products
Observations are rated by risk level and compiled by category.

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

- Example of a risk identified for 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.
- Additional risks are also documented.
On-Site Technical Supplier C-SCRM Assessments
What happens after the initial assessment?

1. Assess
2. Quantify Risks
3. Report and Recommend
4. Improve

Research
On-Site Technical Supplier C-SCRM Assessments Summary

- Another tool for DoD programs to assess and reduce supplier risks
- Suppliers to date have welcomed the results as it has helped them improve their risk posture
- Best prior to acquisition of a major weapon system but applicable at any point in the acquisition lifecycle
USAF Software SBOM R&D Efforts
Initiated our Software SBOM effort…

Because we realized it is the foundation for our Software SCRM effort

Since we will likely need to create SBOMs for our organically developed software once policy matures and wanted to

- provide input to policy that we will eventually need to follow
- establish our own work processes around SBOM before required to
- investigate tools
USAF Software SBOM R&D Efforts
Why SBOM is Important

Create Validated SBOM

Review SBOM and Flag Certain Suppliers for Investigation

Assess Supplier Risks via:
- Intelligence Reports
- Technical Onsite SCRM Assessments
- Business Analytics Reports

Integrate Risks into Program Risk Assessment
USAF Software SBOM R&D Efforts Effort Summary

- The 309 SWEG is actively generating SBOMs, and its members are integrating with the 309th SWEG SCRM IPT:
  - SBOM integration using modern technologies
  - SBOM generation for legacy technologies and systems
  - SBOM collection from upstream suppliers
  - SBOM consumption to find vulnerabilities and adversarial exploits

- Timeline for 309 SWEG SBOM R&D effort
USAF Software SBOM R&D Efforts
Collecting SBOMs

- Establishing a Hardware/Software stack (simulating a Space Force Weapon System stack) to collect SBOMs from firmware and software in the stack
- Participating suppliers: undisclosed but you would recognize them
- Establish SBOM processes

![Diagram of Hardware/Software stack]

- Mission Unique Software
- Real Time Operating System
- Bare Metal Firmware
- Hardware
USAF Software SBOM R&D Efforts

Generating SBOMs

- Experimenting with SBOM generation tools
  - Microsoft SBOM Tool
    - Languages thus far: .Net, Python, C/C++, C#, Java
  - SwiftBOM (CERT)
USAF Software SBOM R&D Efforts Consuming (Analyzing) SBOMs

- Experimenting with SBOM vulnerability identification tools (which use internet-based databases)
  - Daggerboard
  - OWASP Dependency Track
# USAF Software SBOM R&D Efforts

## Notional SBOM Swim Lanes

<table>
<thead>
<tr>
<th>SBOM in a DoD Sw Dev Org</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DEVOPS</td>
</tr>
<tr>
<td></td>
<td>Configuration Management</td>
</tr>
<tr>
<td></td>
<td>Software Assurance</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>System Engineering</td>
</tr>
<tr>
<td></td>
<td>Intelligence</td>
</tr>
<tr>
<td></td>
<td>Enforcement</td>
</tr>
<tr>
<td></td>
<td>Contracting &amp; Acquisitions</td>
</tr>
</tbody>
</table>
USAF Software SBOM R&D Efforts
Notional SBOM Roles in a DoD Program

- 309 SWEG SCRM IPT
  - Developing roles and responsibilities for generation and distribution of SBOMs
  - Minimizing supply chain risks of ingested software

Notional

<table>
<thead>
<tr>
<th>Role</th>
<th>Prime</th>
<th>DoD Sw Dev</th>
<th>DoD PMO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Validate</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Consume</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Generate</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Distribute</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Current Challenges with SBOMs

- No requirement so few suppliers feel compelled to create them or request from their suppliers
- Disconnected networks will require databases updated periodically
- A vulnerability of a software component on an unclassified system often becomes classified requiring special handling
- Suppliers may deem their software proprietary thus limiting access to build-version SBOMs
- Where do we store SBOMS?
- Who has ultimately responsibility for collection, validation, consuming (analyzing) SBOMs? DoD, Services, PMOs?
- …
DoD/NNSA Software Assurance CoP
SBOM WG Update
DoD/NNSA SwA CoP SBOM WG Update

- Team: OSD R&E, MITRE, Aerospace, SEI, DHS/CISA, National Labs, MDA, and the Services
- Effort kicked off at December SwA CoP
- USAF appointed as lead

Tasks:
- Develop a white paper during CY2023 on the SBOM processes and policies needed for both DoD and DoE
  - Provide short-lead policy input during the paper development as requested
- Review and provide input to the SBOM Style Guide v0.1
  - Initiated in OSD XBOM WG
  - Additional input forthcoming as we adapt it from white paper (see below)
SBOM TECHNICAL GUIDANCE & RECOMMENDATIONS

NNSA/DoD Software Assurance Community of Practice

ABSTRACT
Provide Technical guidance and recommendations to senior DoD and DoE leadership in the realm of Software Bill of Materials to assist in policy development and roll out.

SBOM Working Group
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining an SBOM</td>
<td>8</td>
</tr>
<tr>
<td>Current Policy and Guidance References</td>
<td>8</td>
</tr>
<tr>
<td>Recommended Future Policy Language/References</td>
<td>8</td>
</tr>
<tr>
<td>NTIA Standards</td>
<td>8</td>
</tr>
<tr>
<td>Additional DOE/DoD Recommended Information</td>
<td>9</td>
</tr>
<tr>
<td>Acquiring SBOMs of Software Products</td>
<td>10</td>
</tr>
<tr>
<td>Current Policy and Guidance References</td>
<td>10</td>
</tr>
<tr>
<td>Recommended Future Policy Language/References</td>
<td>10</td>
</tr>
<tr>
<td>Technical Findings</td>
<td>10</td>
</tr>
<tr>
<td>Generation</td>
<td>11</td>
</tr>
<tr>
<td>Current Policy and Guidance References</td>
<td>11</td>
</tr>
<tr>
<td>Recommended Future Policy Language/References</td>
<td>11</td>
</tr>
<tr>
<td>Technical Findings</td>
<td>11</td>
</tr>
<tr>
<td>Storage</td>
<td>12</td>
</tr>
<tr>
<td>Current Policy and Guidance References</td>
<td>12</td>
</tr>
<tr>
<td>Recommended Future Policy Language/References</td>
<td>12</td>
</tr>
<tr>
<td>Technical Findings</td>
<td>12</td>
</tr>
<tr>
<td>Sharing</td>
<td>13</td>
</tr>
<tr>
<td>Current Policy and Guidance References</td>
<td>13</td>
</tr>
<tr>
<td>Recommended Future Policy Language/References</td>
<td>13</td>
</tr>
<tr>
<td>Technical Findings</td>
<td>13</td>
</tr>
<tr>
<td>Consumption</td>
<td>14</td>
</tr>
</tbody>
</table>
Contact Us

➢ Parker Bauer
  ➢ parker.bauer@us.af.mil
  ➢ (801) 777-5308

➢ Alexander Wright
  ➢ alexander.wright.4@us.af.mil
  ➢ (720) 648-8694
Discussion