Lifecycle Assessment Approach for Supply Chain Risk

Carol Woody, Ph.D.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Supply Chain Risk Management: *Intentional and Unintentional Acts*

**Intentional acts**
- counterfeit hardware and software
- malware insertion

**Unintentional acts**
- poor code quality
- software vulnerabilities unintentionally inserted

**Result:** Systems with adverse behaviors
Risks Come from Unexpected Sources

Manufacturing and Integration Supply Chains: responsible for conceptualizing, designing, building and delivering systems and hardware

Service Supply Chains: responsible for providing services to acquirers including data processing and hosting, logistical services, and support for administrative functions

Software Supply Chains: responsible for producing the software that runs on vital systems
Steel furnaces have been successfully attacked

“Steelworks compromise causes massive damage to furnace.

One of the most concerning was a targeted APT attack on a German steelworks which ended in the attackers gaining access to the business systems and through them to the production network (including SCADA). The effect was that the attackers gained control of a steel furnace and this caused massive damages to the plant.”

Service Supply Chains

11 gigabytes (GB) of data - 110,000,000 records worth of payments, transactions, and other personally identifiable data stolen

Target Stores Attacked through Service Support

• Heating and cooling service (HVAC) vendor is compromised
• Target store network achieved through HVAC remote access
• Malware injects itself into running Point of Sale processes to identify credit card track data and copy it prior to encryption
• Stolen data transmitted to a File Transfer Protocol (FTP) server belonging to a hijacked website
• Criminals then downloaded the data files from the FTP server

SSCA
August 29, 2017
© 2017 Carnegie Mellon University
Software Supply Chains

Software Vulnerabilities Enable Attacks

Newkirk Products, a ID card provider for health insurance organizations, is notifying 3.3 million people that their personal data were compromised (May 2016).

Widely used open source software with vulnerabilities that were exploited.

46 million vulnerable open source components downloaded annually.
Government Acquisition Carries Risk

Fifty intrusions or cyber events targeted TRANSCOM contractors between June 2012 and May 2013. Exposed sensitive information on the movement of troops and equipment, potentially disrupting military operations.

At least 20 were successful but TRANSCOM was only told about 2. Contractor reporting requirements were changed after an investigation.

Development Is Now Assembly

Collective development – context:
• Too large for single organization
• Too much specialization
• Too little value in individual components

Note: hypothetical application composition
Supply Chains are Long (often obscure) Paths

Open Source Example

- App server
- HTTP server
- XML Parser
- C Libraries
- C compiler
- Generated Parser
- Parser Generator
- 2nd Compiler
Supply Chain Relationships are Complex
Monitor SCRM Risk Factors (SPDO)

Claim: Software supply chain risk for a product has been reduced to acceptable level

- **Evidence of Supplier Capability**: Supplier follows practices that reduce supply chain risks
- **Evidence of Product Security**: Delivered or updated product is acceptably secure
- **Evidence of Product Distribution**: Methods of transmitting the product to the purchaser guard against tampering
- **Evidence of Operational Product Control**: Product is used in a secure manner

Supply Chain Risk Management: Acquisition Security Framework (ASF)

**What**
- Assess gaps in a program’s supply chain practices that can lead to cybersecurity risk

**Why**
- Organizations can inherit cybersecurity risks from third-party products and services.

**Benefits**
- Provides the basis for improving a program’s supply chain practices
- Reduces cybersecurity risk of deployed software-reliant systems
ASF: Practice Areas

1. Relationship Formation
2. Relationship Management and Governance
3. Engineering
4. Secure Product Operation and Sustainment
5. Supply Chain Technology Infrastructure
## ASF Practice Areas Map to SCRM Risk Factors

<table>
<thead>
<tr>
<th>Practice Area</th>
<th>Supplier Capability</th>
<th>Product Security</th>
<th>Product Distribution</th>
<th>Operational Product Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Relationship Formation</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Relationship Management and Governance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Engineering</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>4. Secure Product Operation and Sustainment</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>5. Supply Chain Technology Infrastructure</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Supply Chain Decisions Add to Software Faults

Where Software Flaws Are Introduced

- Requirements Engineering: 70%
- System Design: 20%
- Software Architectural Design: 10%
- Component Software Design: 3.5%
- Code Development: 16%
- Unit Test: 50.5%
- Integration: 9%
- System Test: 21%
- Acceptance Test: 9%
- Operation: 21%

Where Software Flaws Are Found

Improved focus on SCRM activities needed on the front-in of the SDLC

Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies
Software Faults: *Introduction, Discovery, and Cost*

Faults account for 30–50% percent of total software project costs.
- Most faults are introduced before coding (~70%).
- Most faults are discovered at system integration or later (~80%).

**Software Development Lifecycle**

<table>
<thead>
<tr>
<th>Where Faults are Introduced</th>
<th>Where Faults are Found</th>
<th>Nominal Cost Per Fault for Fault Removal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>70%</strong> Requirements Engineering</td>
<td><strong>3.5%</strong></td>
<td><strong>300–1000x</strong></td>
</tr>
<tr>
<td><strong>20%</strong> System Design</td>
<td><strong>16%</strong></td>
<td></td>
</tr>
<tr>
<td><strong>10%</strong> Software Architectural Design</td>
<td><strong>50.5%</strong></td>
<td></td>
</tr>
<tr>
<td>Component Software Design</td>
<td><strong>9%</strong></td>
<td></td>
</tr>
<tr>
<td>Code Development</td>
<td><strong>20.5%</strong></td>
<td></td>
</tr>
</tbody>
</table>
Improvement Starts with an ASF Review

Identify, prioritize, and mitigate gaps in a program’s supply chain practices that can lead to cybersecurity risk

Next steps for SEI research:
• build out detailed practices for ASF
• work with selected pilot organizations to refine and improve review processes
Additional Material

CrossTalk
May/June 2017

Contact Information

Carol Woody
chwoddy@cert.org

Web Resources
(CERT/SEI)
http://www.sei.cmu.edu/