Lifecycle Assessment Approach for Supply Chain Risk

Carol Woody, Ph.D.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

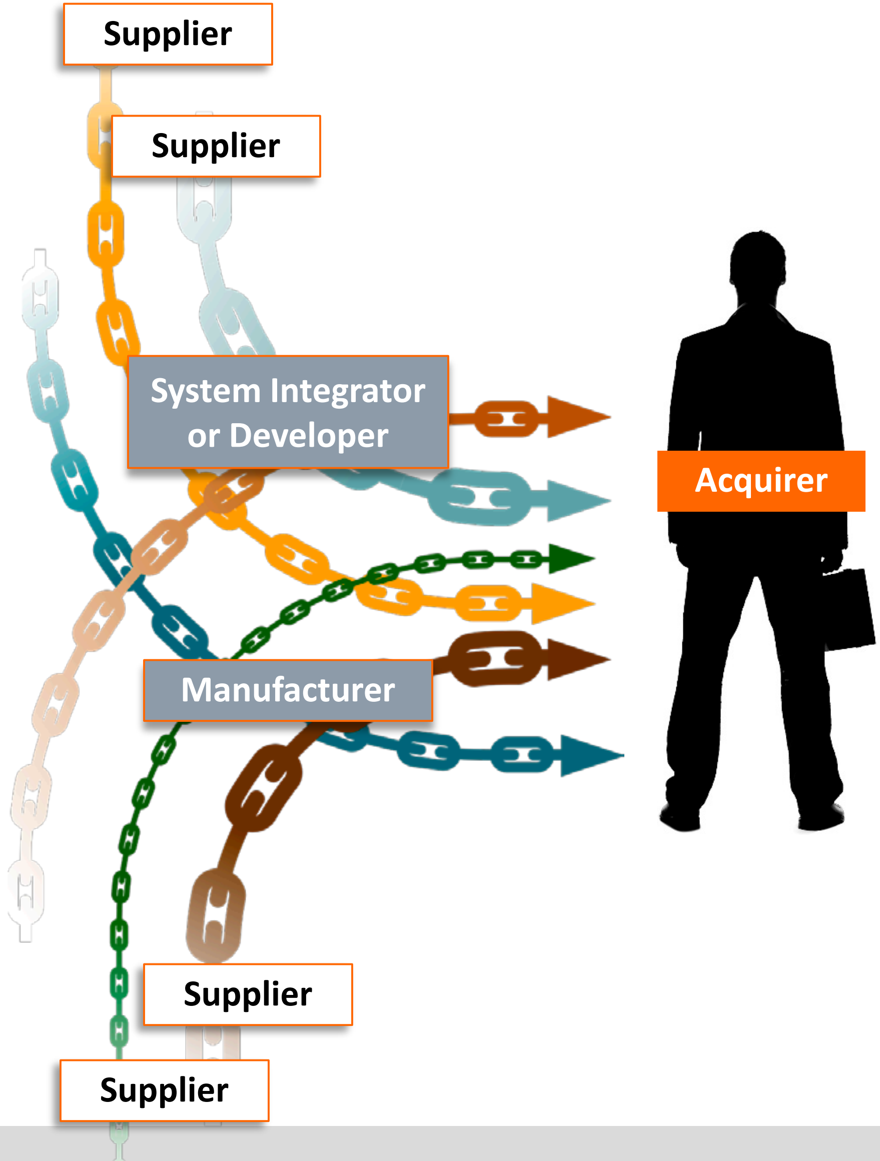
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM17-0559

Supply Chain Risk Management: *Intentional and Unintentional Acts*



Intentional acts

- counterfeit hardware and software
- malware insertion

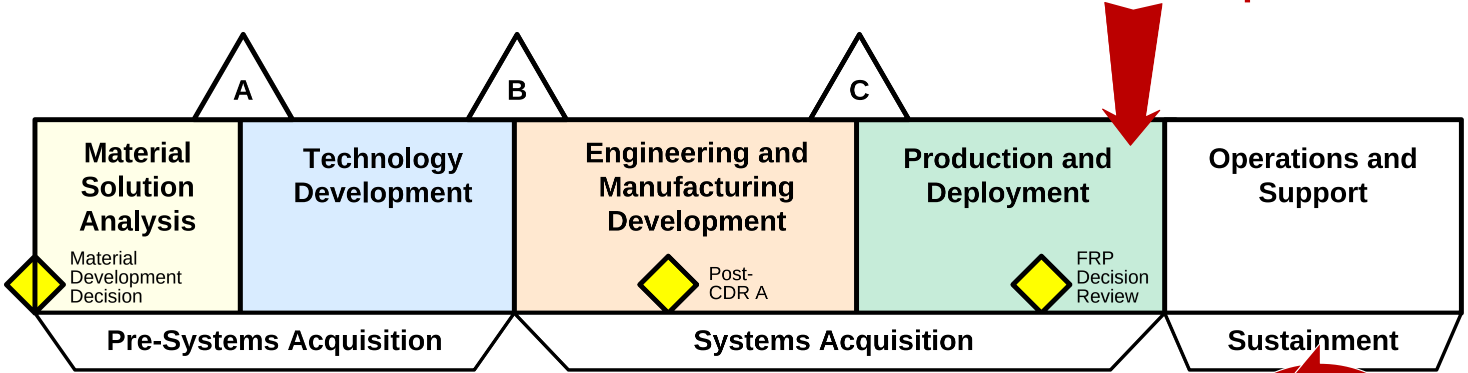
Unintentional acts

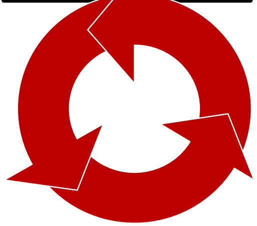
- poor code quality
- software vulnerabilities unintentionally inserted

Result: Systems with adverse behaviors

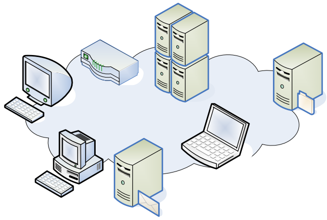
Software Assurance Landscape: System Lifecycle

Certification and Authorization to Operate

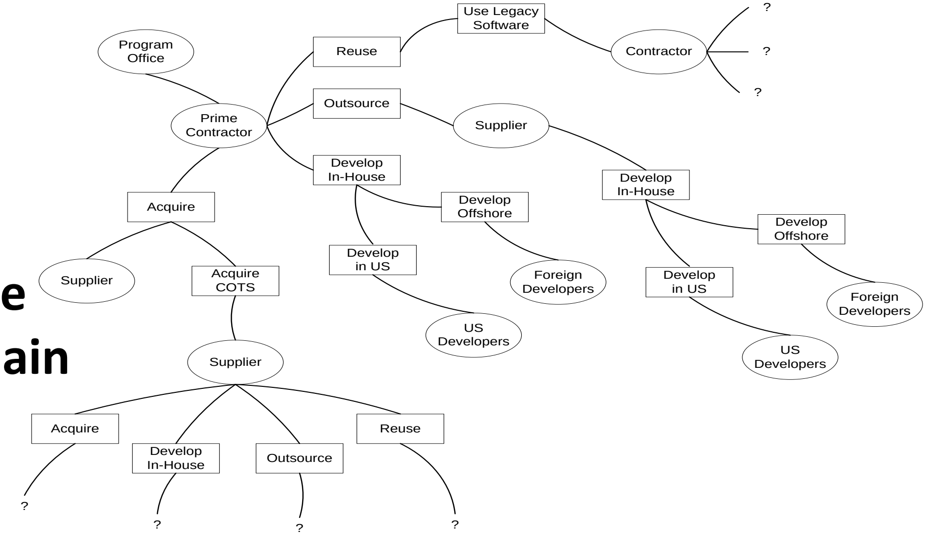




Software Patch Cycle



Software Supply Chain



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

Manufacturing and Integration Supply Chains

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.”

Source: Sources: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile; http://www.resilienceoutcomes.com/state-ict-security/

Service Supply Chains

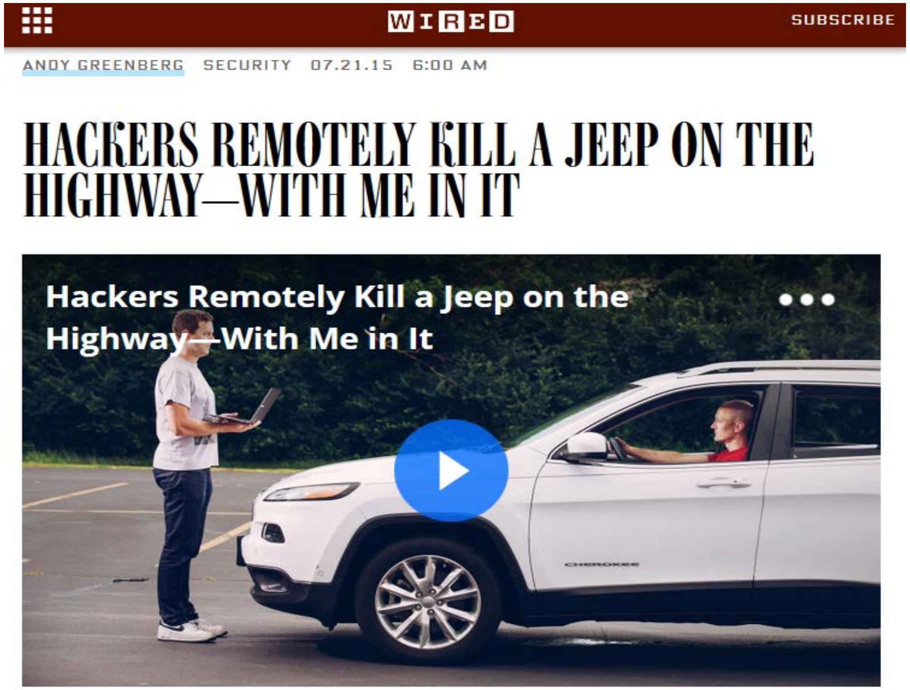
11 gigabytes (GB) of data - 110,000,000 records worth of payments, transactions, and other personally identifiable data stolen

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

Software Supply Chains

Software Vulnerabilities Enable Attacks



WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

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 with vulnerabilities that were exploited

46 million vulnerable open source components downloaded annually

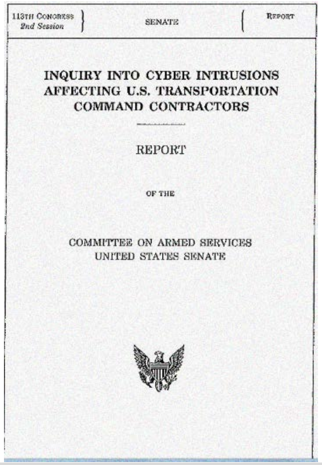
Government Acquisition Carries Risk

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.

https://defensesystems.com/articles/2014/09/18/us-transcom-china-contractor-hacks.aspx



113TH CONGRESS
2nd Session

SENATE

REPORT

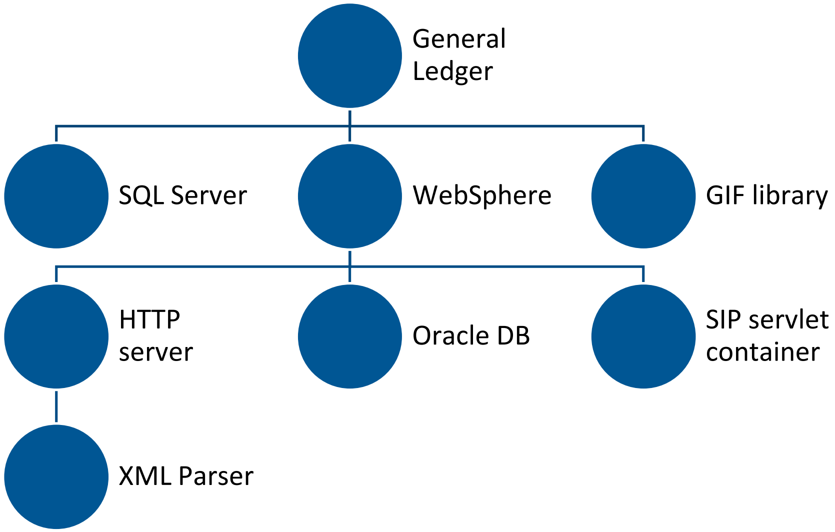
INQUIRY INTO CYBER INTRUSIONS AFFECTING U.S. TRANSPORTATION COMMAND CONTRACTORS

REPORT

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

Development Is Now Assembly

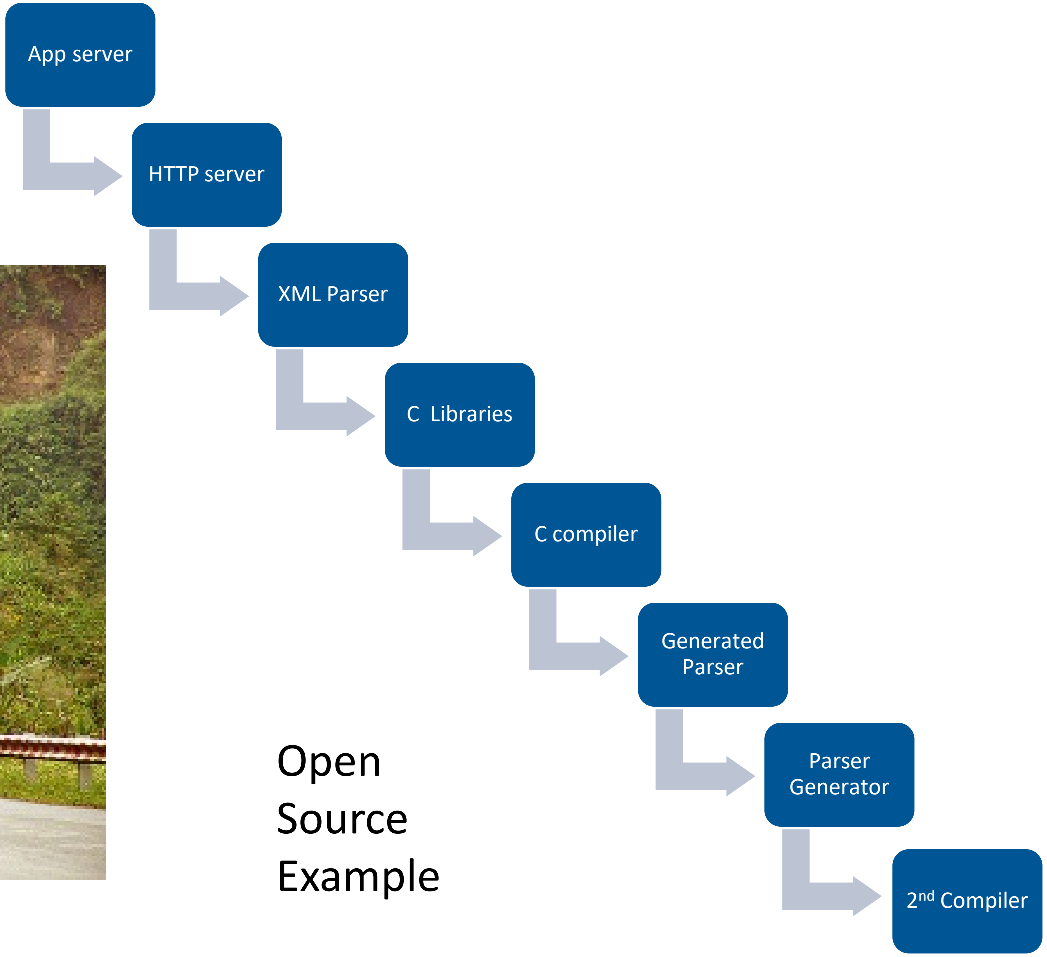


Collective development – context:

- 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



App server

HTTP server

XML Parser

C Libraries

C compiler

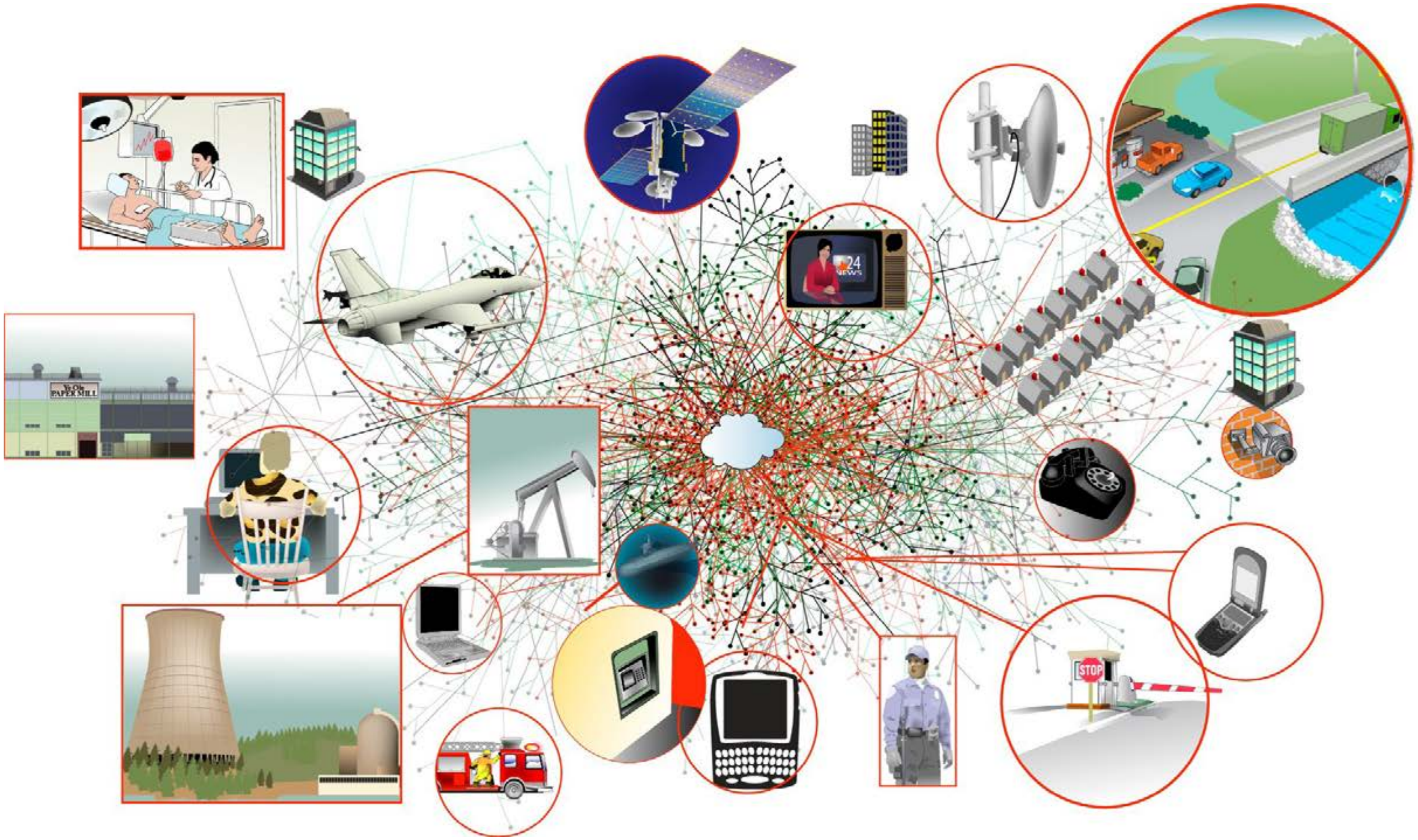
Generated Parser

Parser Generator

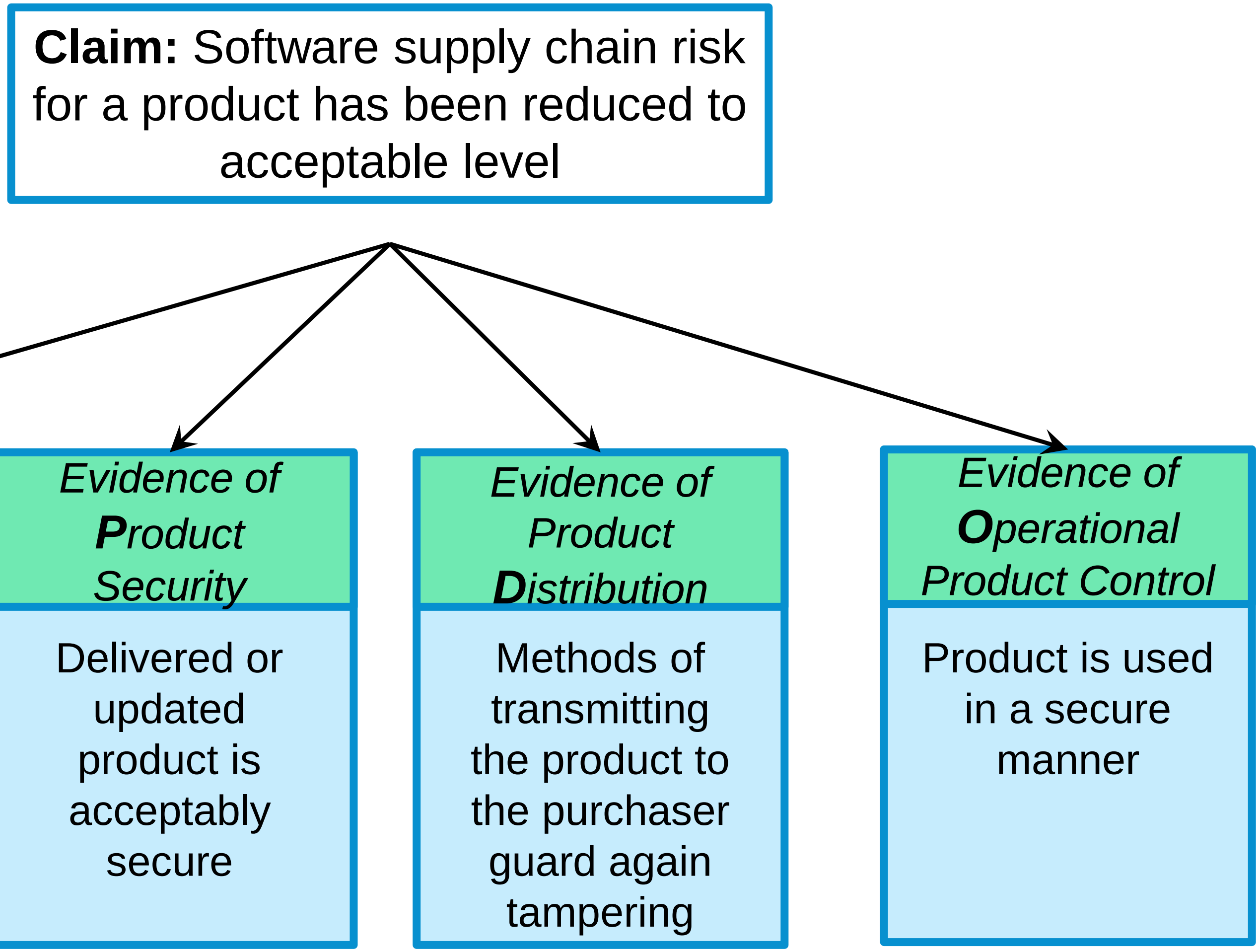
2nd Compiler

Open
Source
Example

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 **S**upplier Capability*

Supplier follows practices that reduce supply chain risks

*Evidence of **P**roduct Security*

Delivered or updated product is acceptably secure

*Evidence of Product **D**istribution*

Methods of transmitting the product to the purchaser guard again tampering

*Evidence of **O**perational Product Control*

Product is used in a secure manner

Evaluating and Mitigating Software Supply Chain Security Risks http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9337

Supply Chain Risk Management: Acquisition Security Framework (ASF)

What

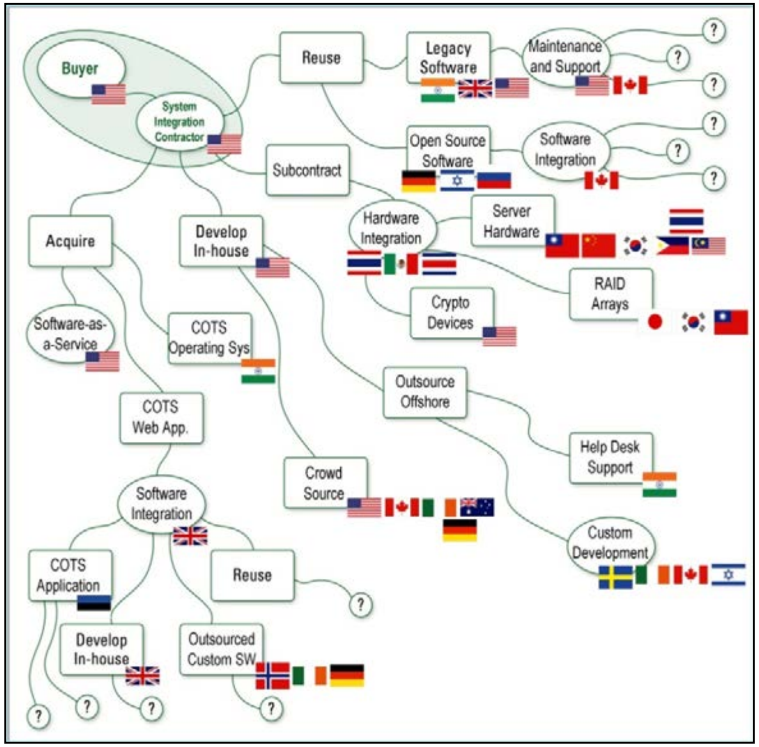
- Assess gaps in a program’s supply chain practices that can lead to cybersecurity risk

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



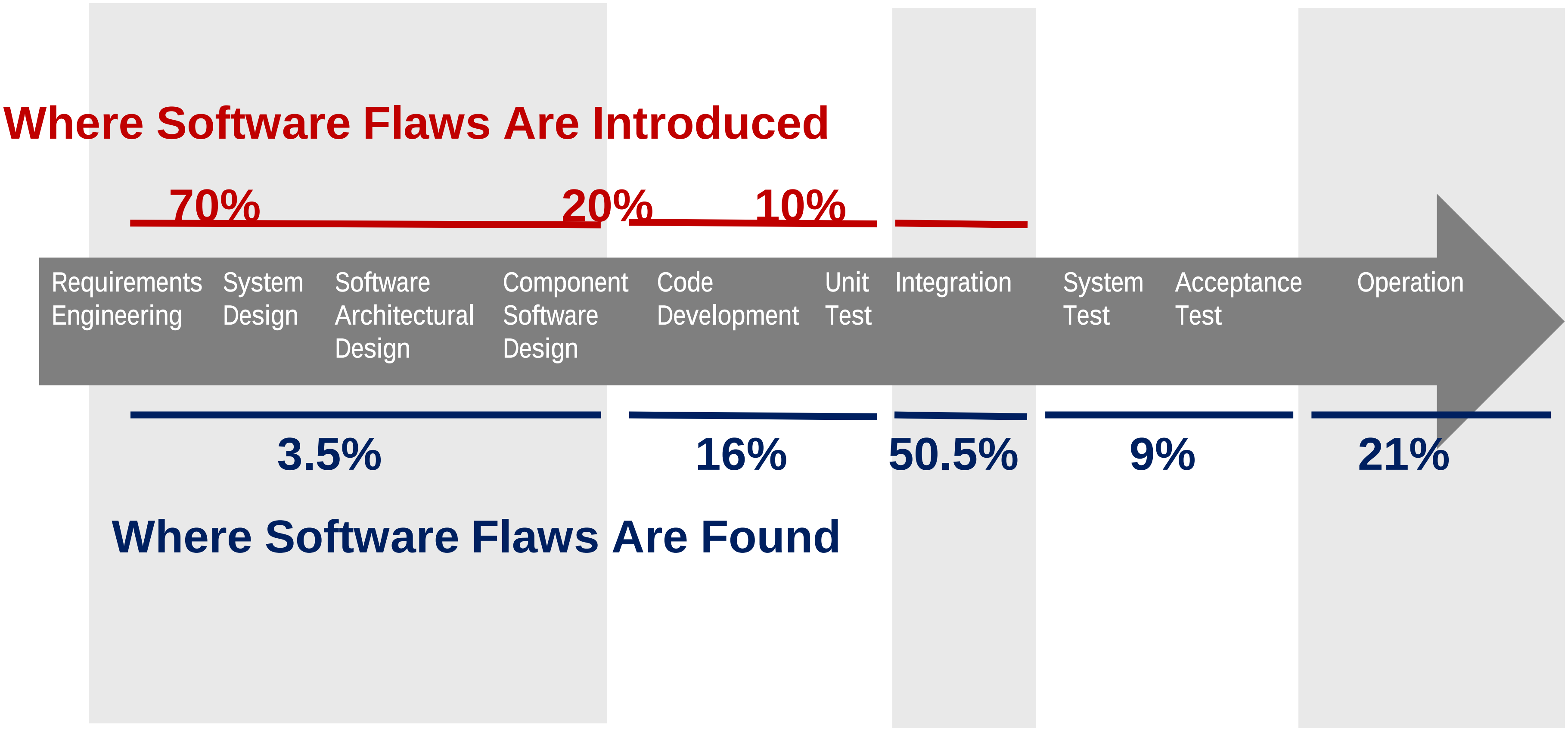
ASF: Practice Areas

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

	Supplier Capability	Product Security	Product Distribution	Operational Product Control
1. Relationship Formation	X			
2. Relationship Management and Governance	X			
3. Engineering		X	X	
4. Secure Product Operation and Sustainment				X
5. Supply Chain Technology Infrastructure	X	X	X	X

Supply Chain Decisions Add to Software Faults



Where Software Flaws Are Introduced

70% 20% 10%

Requirements Engineering | System Design | Software Architectural Design | Component Software Design | Code Development | Unit Test | Integration | System Test | Acceptance Test | Operation

3.5% 16% 50.5% 9% 21%

Where Software Flaws Are Found

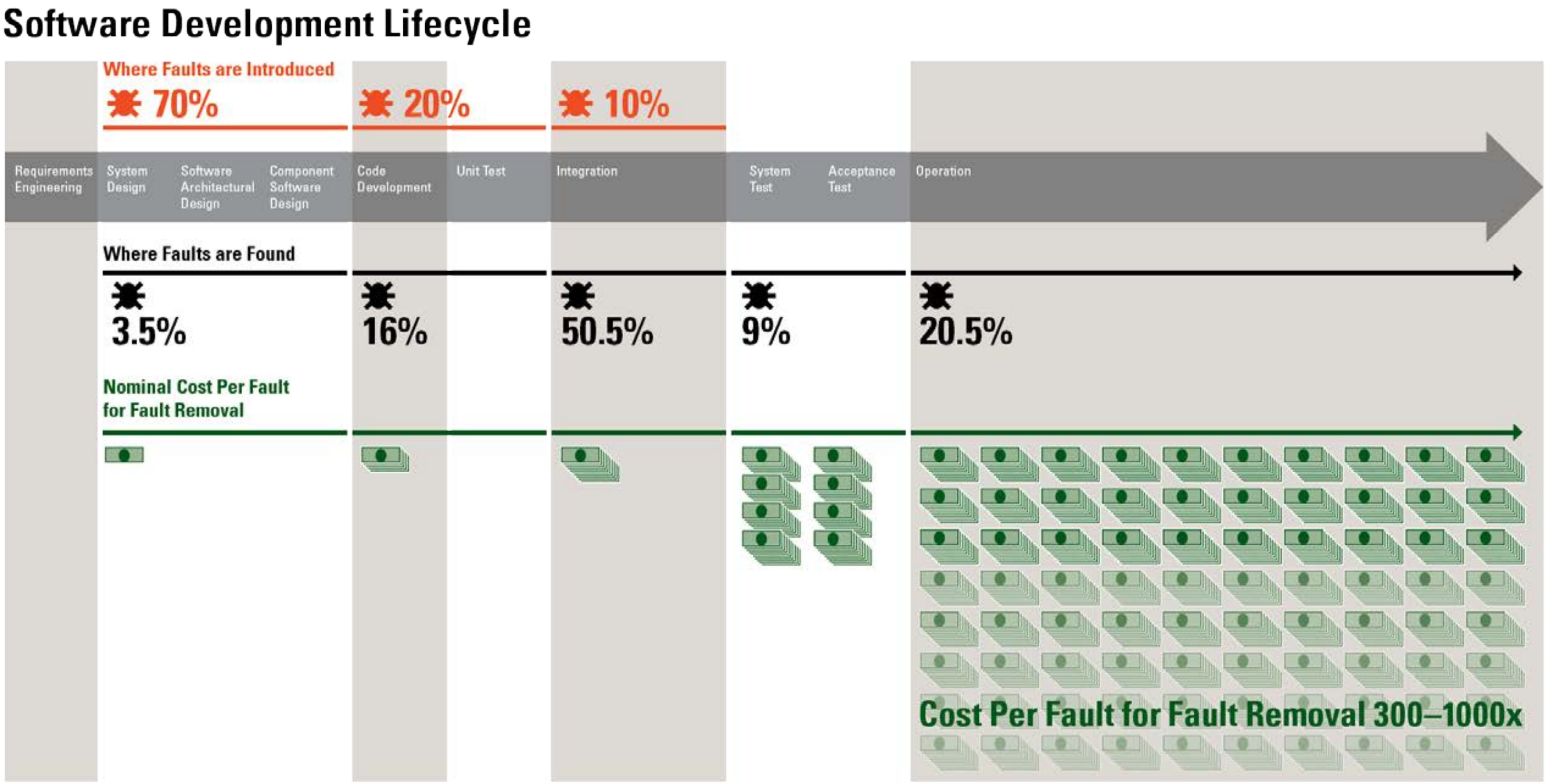
Improved focus on SCRM activities needed on the front-in of the SDLC

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%).



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

http://static1.1.sqspcdn.com/static/f/702523/27545065/1493612336550/201705-Alberts.pdf?token=SIsZ2ZB1KHteEggqCl%2F%2Fv5Rz780%3D

Contact Information

Carol Woody
cwoody@cert.org

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