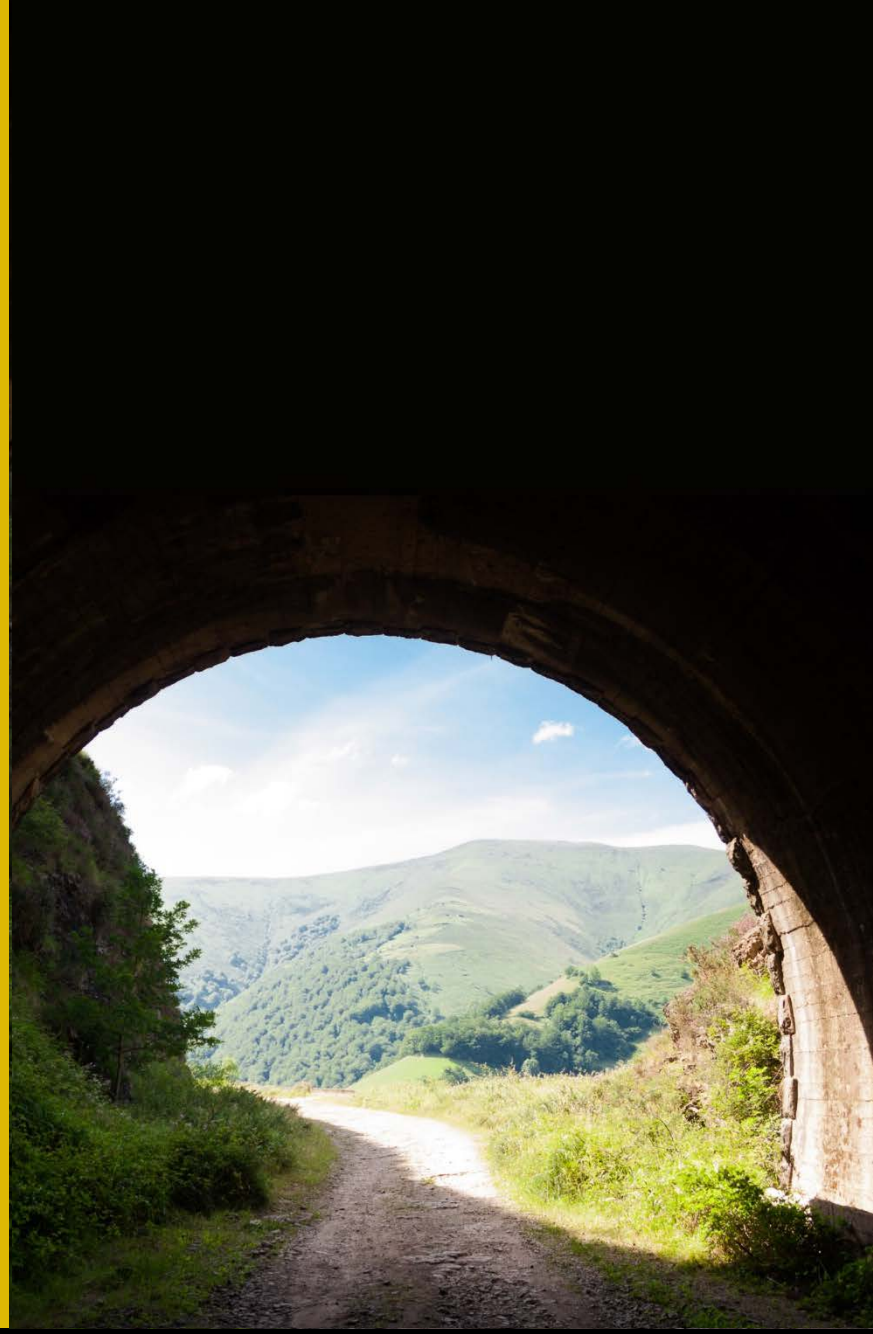
Supply Chain Risk Management - Introduction



Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0660

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Information and Communication Technology (ICT)

Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information[1]

- Comprises many components, including microelectronics, computing systems, networks, software, and mobile devices
- Relies on a complex, globally distributed, and interconnected supply chain ecosystem that is long, has geographically diverse routes, and consists of multiple tiers of outsourcing

1. National Institute of Standards and Technology. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (NIST Special Publication 800-161). Gaithersburg, MD, National Institute of Standards and Technology, 2015.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

ICT Supply Chain

Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer[1]

The distributed and interconnected ecosystem of people, processes, technologies, information, and resources required to create and deliver a product or service

1. National Institute of Standards and Technology. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (NIST Special Publication 800-161). Gaithersburg, MD, National Institute of Standards and Technology, 2015.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

ICT Supply Chain Complexity

An organization's supply chains often span multiple countries.

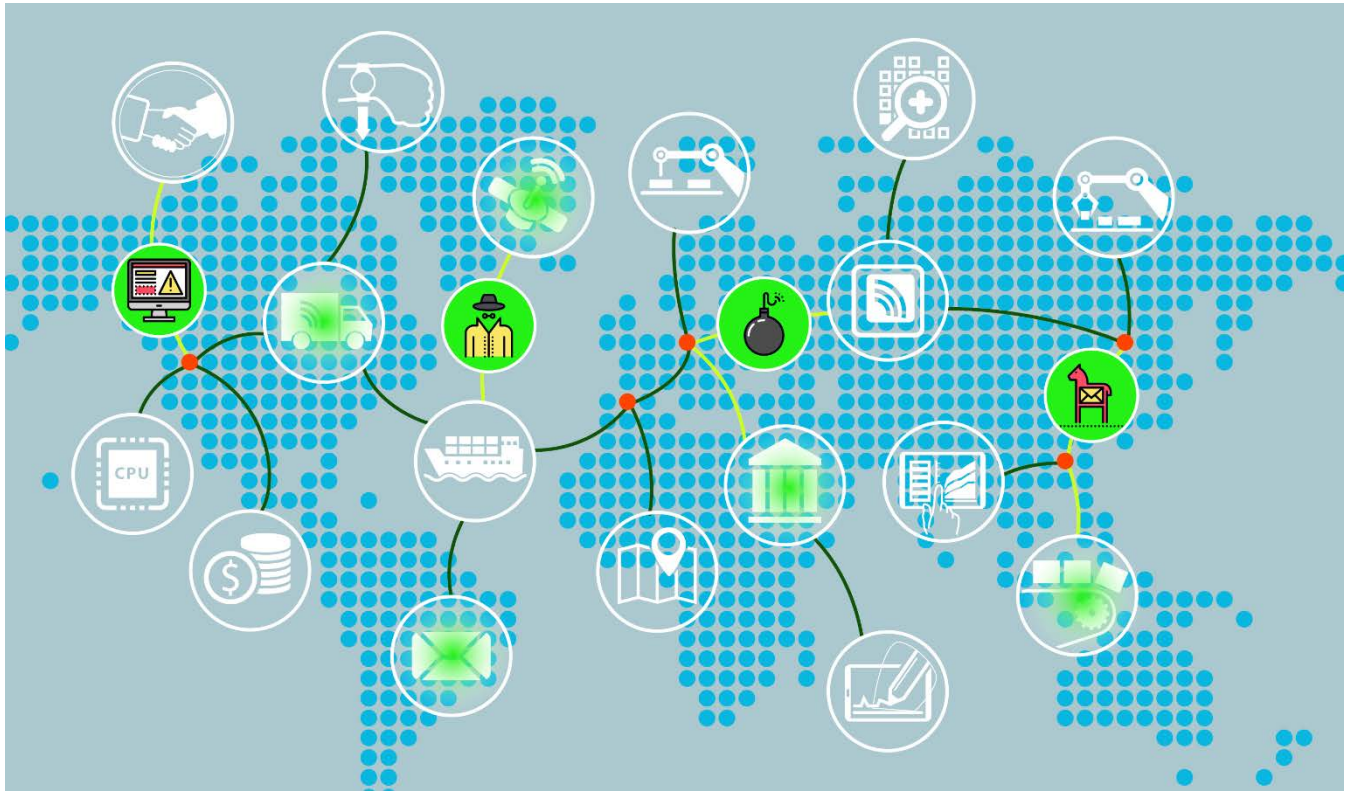
ICT supply chains are dynamic, multi-tiered, and complex, making it difficult for an organization to view all layers of its supply chain.

Components that end up in an ICT product have their own supply chains.

The lack of visibility and traceability of ICT supply chains can lead to security risks.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

ICT Supply Chain Risk



Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation[1]

ICT supply chain risks are realized when threats in the ICT supply chain exploit existing vulnerabilities.

1. National Institute of Standards and Technology. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (NIST Special Publication 800-161). Gaithersburg, MD, National Institute of Standards and Technology, 2015.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Examples of ICT Supply Chain Risks[1]

Insertion of counterfeits

Unauthorized production

Tampering

Theft of software, computing capability and data

Insertion of malicious software and hardware (e.g., GPS tracking devices, computer chips, etc.)

Poor manufacturing and development practices in the ICT supply chain

1. National Institute of Standards and Technology. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (NIST Special Publication 800-161). Gaithersburg, MD, National Institute of Standards and Technology, 2015.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

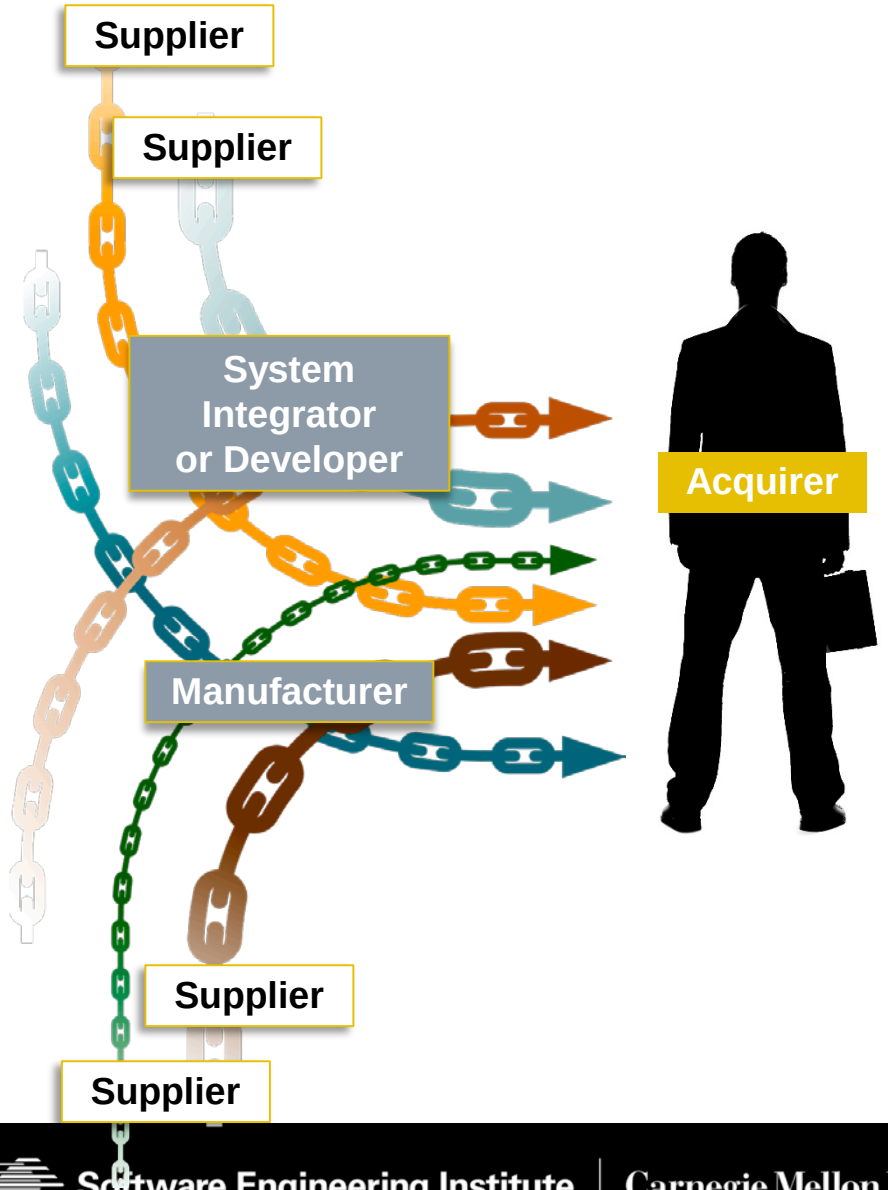
ICT Supply Chain Risk Management

The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains[1]

1. National Institute of Standards and Technology. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (NIST Special Publication 800-161). Gaithersburg, MD, National Institute of Standards and Technology, 2015.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

ICT Supply Chain Threats



ICT components are susceptible to intentional and unintentional threats.

Intentional threats

- counterfeit hardware and software
- tampering
- theft
- malware insertion

Unintentional threats

- poor code quality
- software vulnerabilities unintentionally inserted

Result: Systems with adverse behaviors

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

ICT Supply Chain Vulnerabilities[1]

ICT supply chain vulnerabilities may be found in

- The systems/components within the SDLC (i.e., being developed and integrated)
- The development and operational environment directly impacting the SDLC
- The logistics/delivery environment that transports ICT systems and components (logically or physically)

1. National Institute of Standards and Technology. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (NIST Special Publication 800-161). Gaithersburg, MD, National Institute of Standards and Technology, 2015.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Types of ICT Supply Chains

Hardware Supply Chains

- Conceptualize, design, build, and deliver hardware and systems
- Includes manufacturing and integration supply chains

Service Supply Chains

- Provide services to acquirers, including data processing and hosting, logistical services, and support for administrative functions

Software Supply Chains

- Produce the software that runs on vital systems
- Comprise the network of stakeholders that contribute to the content of a software product or that have the opportunity to modify its content

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

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

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Service Supply Chains

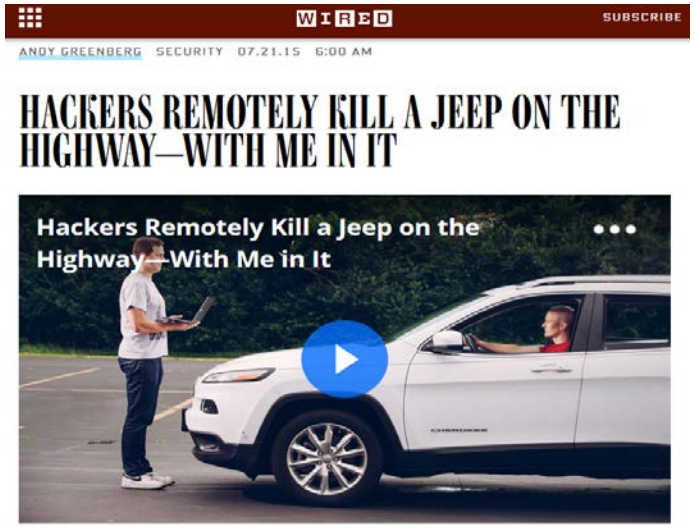
11 gigabytes (GB) of data - 110,000,000 records' worth of payments, transactions, and other personally identifiable data stolen

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

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software Vulnerabilities Enable Attacks



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

HeartBleed and ShellShock are attacks that exploited vulnerabilities in widely used open source software

46 million vulnerable open source components are downloaded annually

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Focus of this Course: *Software Supply Chains*

This course is primarily focused on managing software supply chains as part of an organization's software assurance practice.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software Assurance

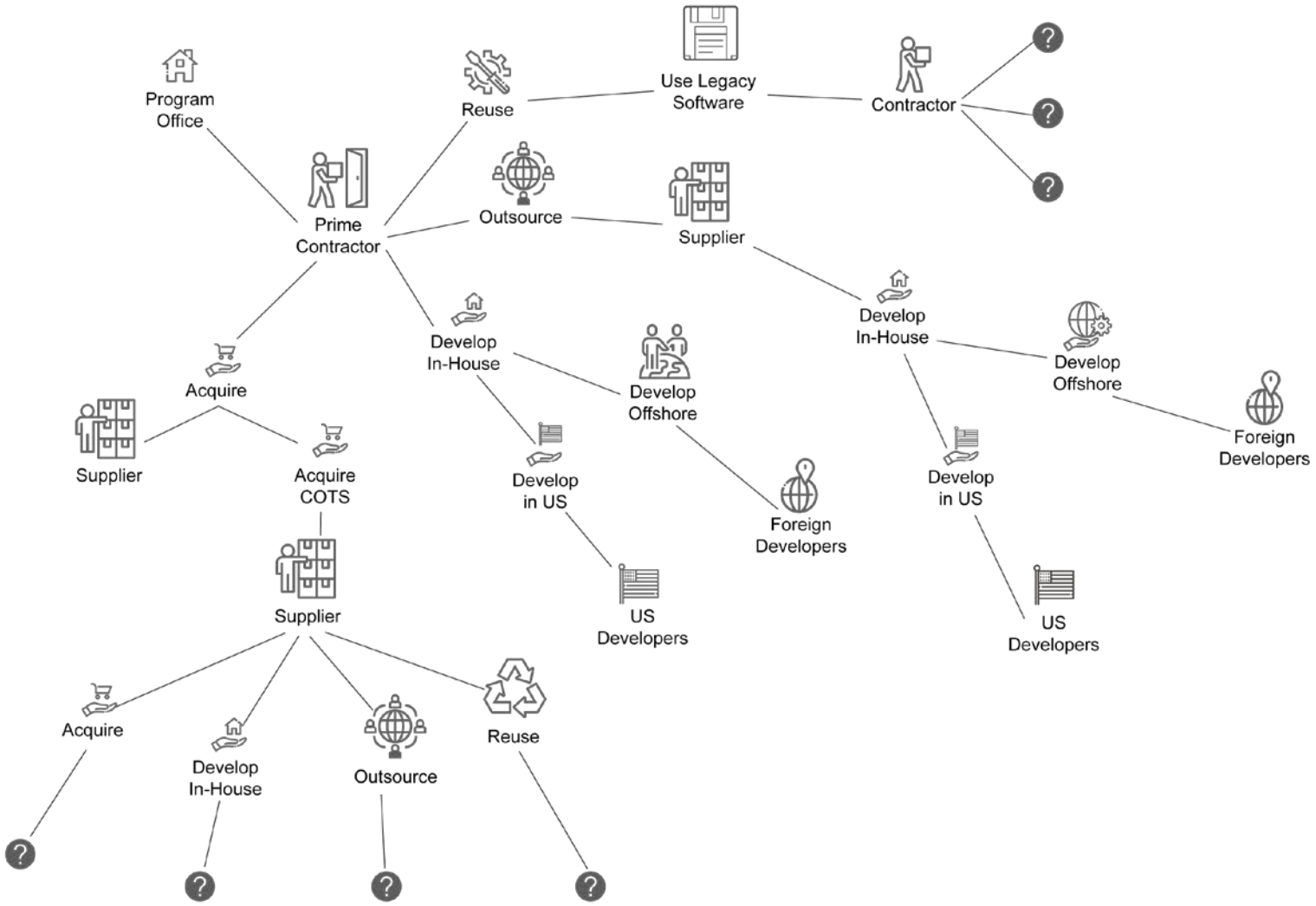
Software assurance is defined as a level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the lifecycle.[1]

Software assurance is becoming increasingly important to organizations across all sectors because of software's increasing influence in business- and mission-critical systems.

1. One Hundred Twelfth Congress of the United States of America. *National Defense Authorization Act for Fiscal Year 2013*. Washington, DC, 2013. http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Types of Software



Commercial-off-the-shelf (COTS) software

Open source software

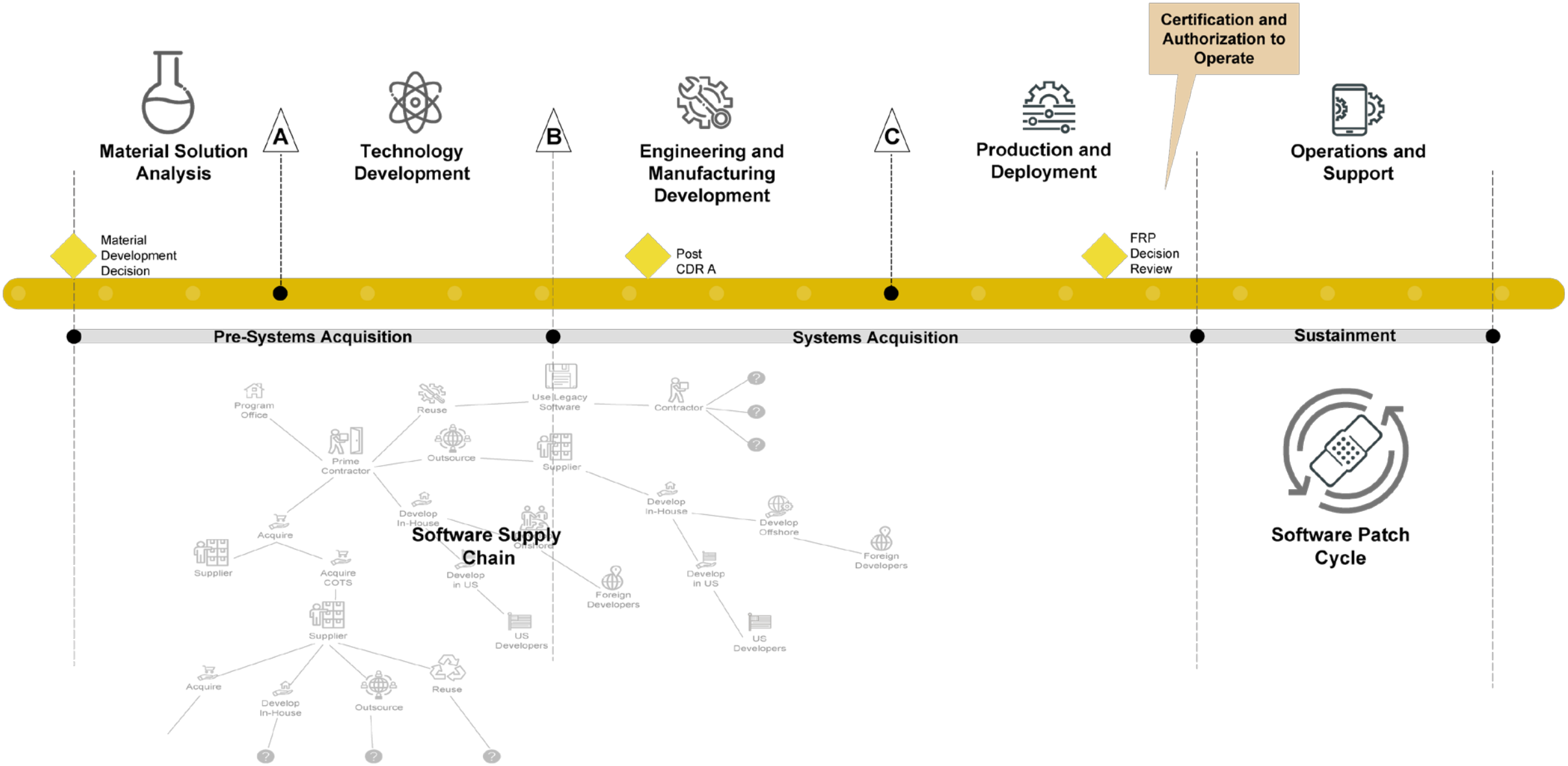
Custom-developed software

Software as a service (SaaS)

Software-reliant systems
(e.g., cyber-physical products)

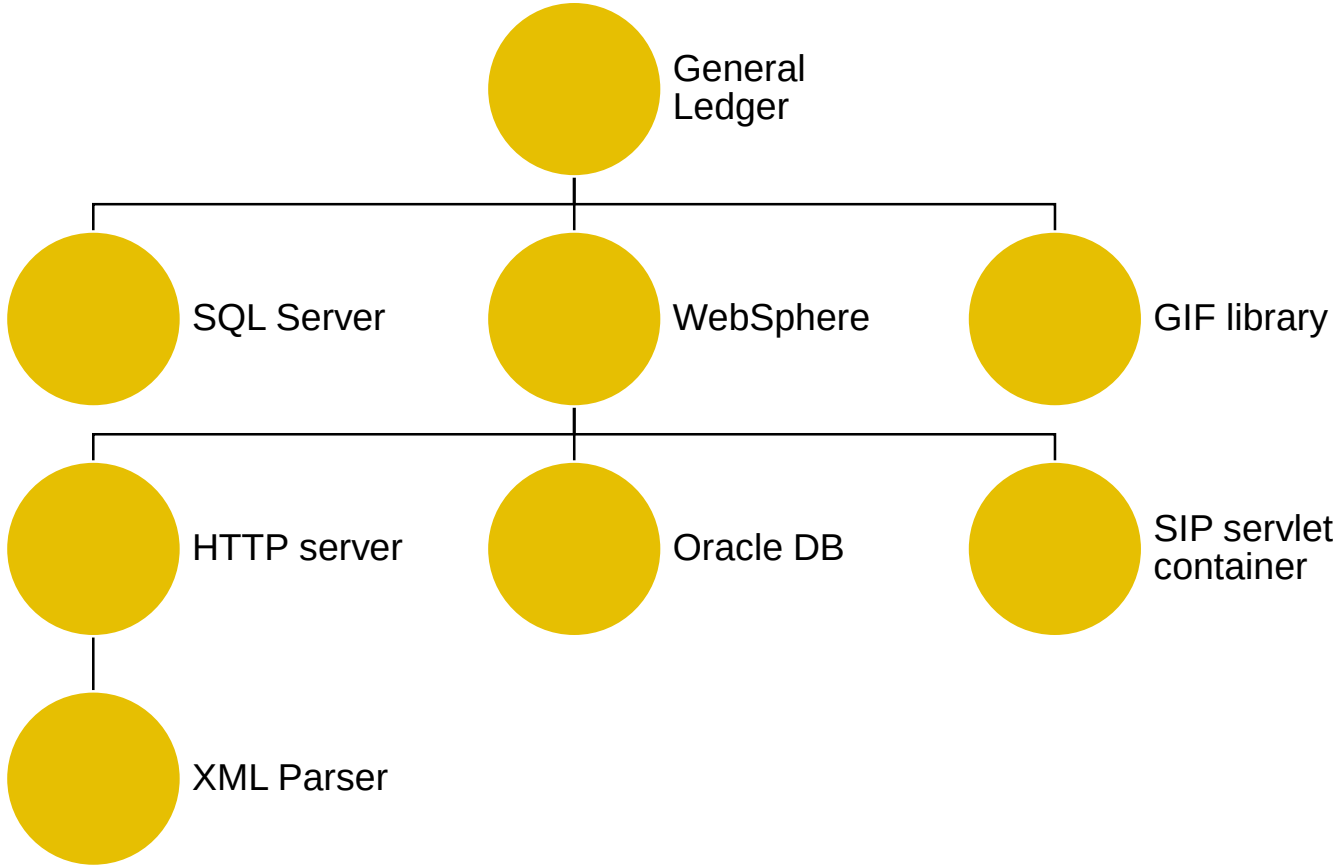
© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software Assurance Landscape: System Lifecycle



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software Development Is Now Assembly



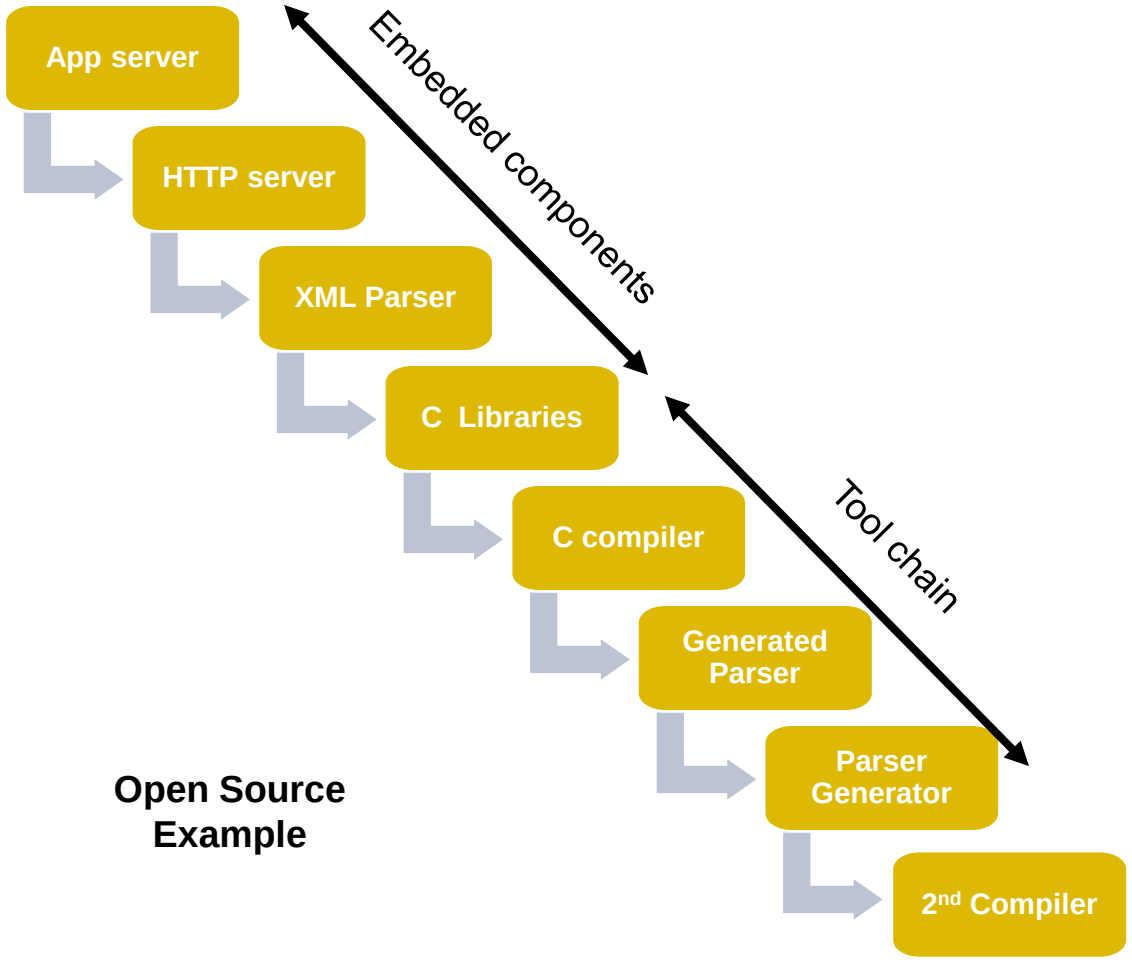
Collective development – context:

- Too large for single organization
- Too much specialization
- Too little value in individual components

Note: hypothetical application composition

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

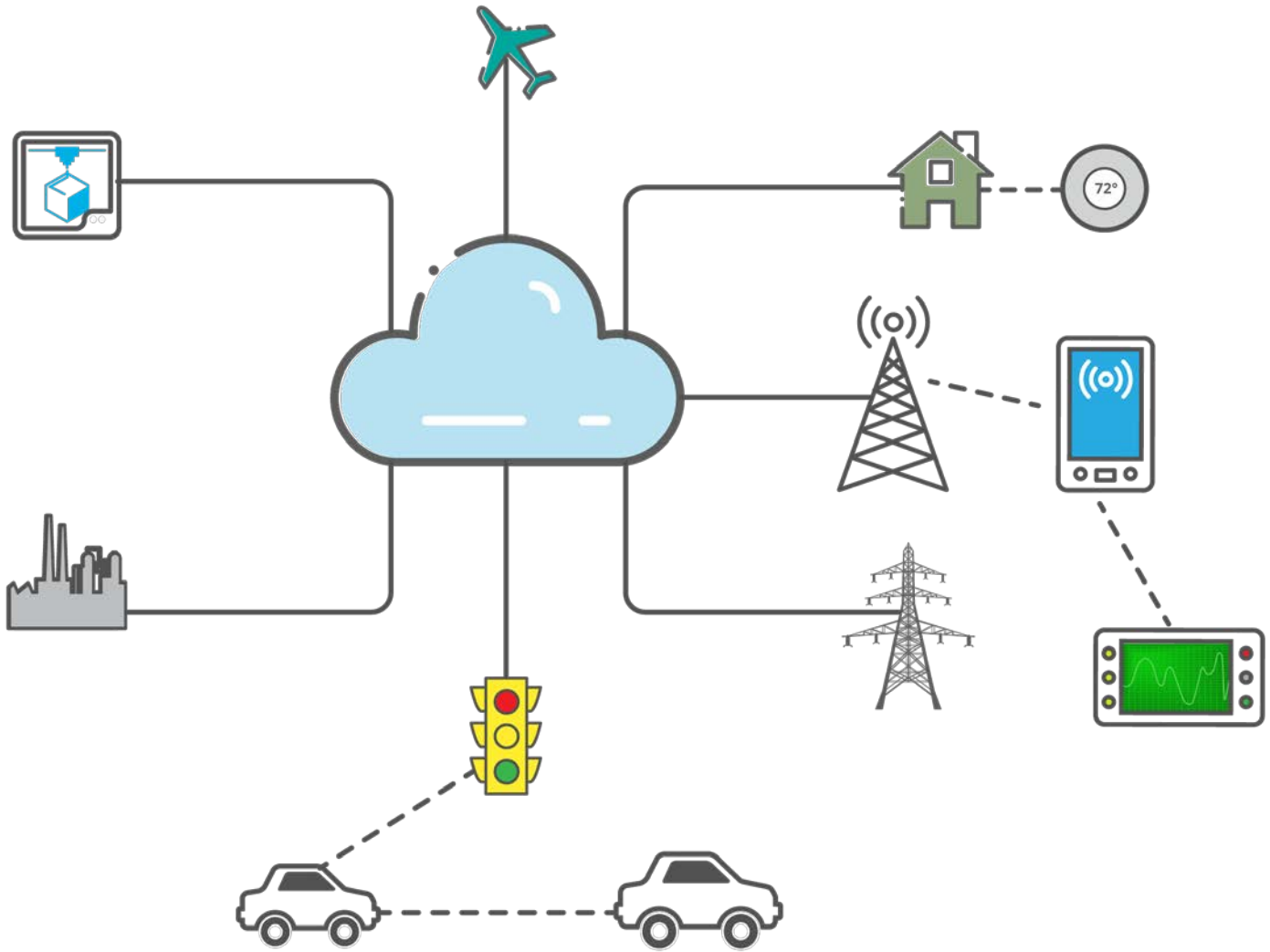
Software Sources are Many, Varied, Reusable



Open Source Example

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

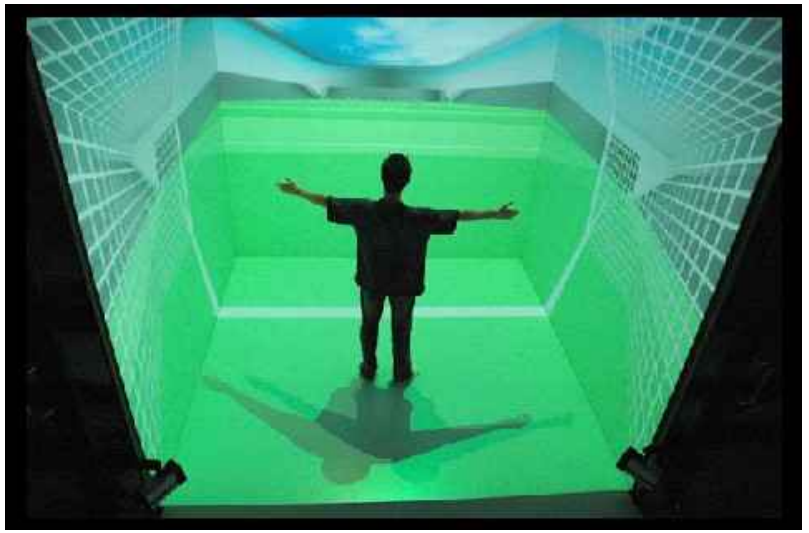
Software Connecting and Communicating Grows



- Cellular
  - Main processor
  - Graphics processor
  - Baseband processor (SDR)
  - Secure element (SIM)
- Automotive
  - Autonomous vehicles
  - Vehicle to infrastructure (V2I)
  - Vehicle to vehicle (V2V)
- Industrial and home automation
  - 3D printing (additive manufacturing)
  - Autonomous robots
  - Interconnected SCADA
- Aviation
  - Next Gen air traffic control
  - Fly by wire
- Smart grid
  - Smart electric meters
  - Smart metering infrastructure
- Embedded medical devices

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software is the New Hardware



Information Technology (IT) is moving from specialized hardware to software, virtualized as

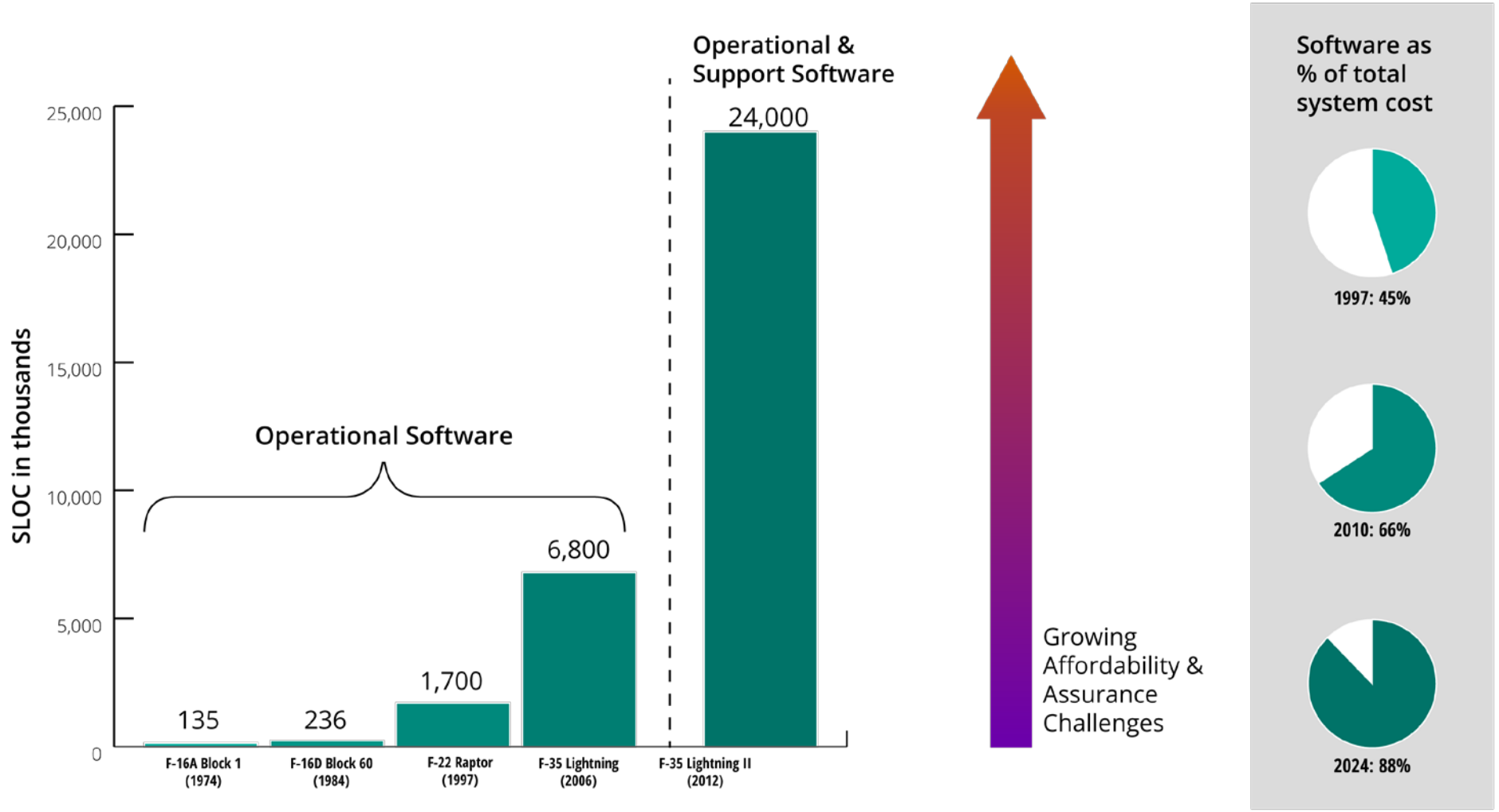
- Servers: virtual Central Processing Units (CPUs)
- Storage: Storage Area Networks (SANs)
- Switches: Soft switches
- Networks: Software defined networks

Scalable cloud computing environments are replacing organization-owned data centers

Firmware, which can be updated, provides the low-level program control for hardware

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

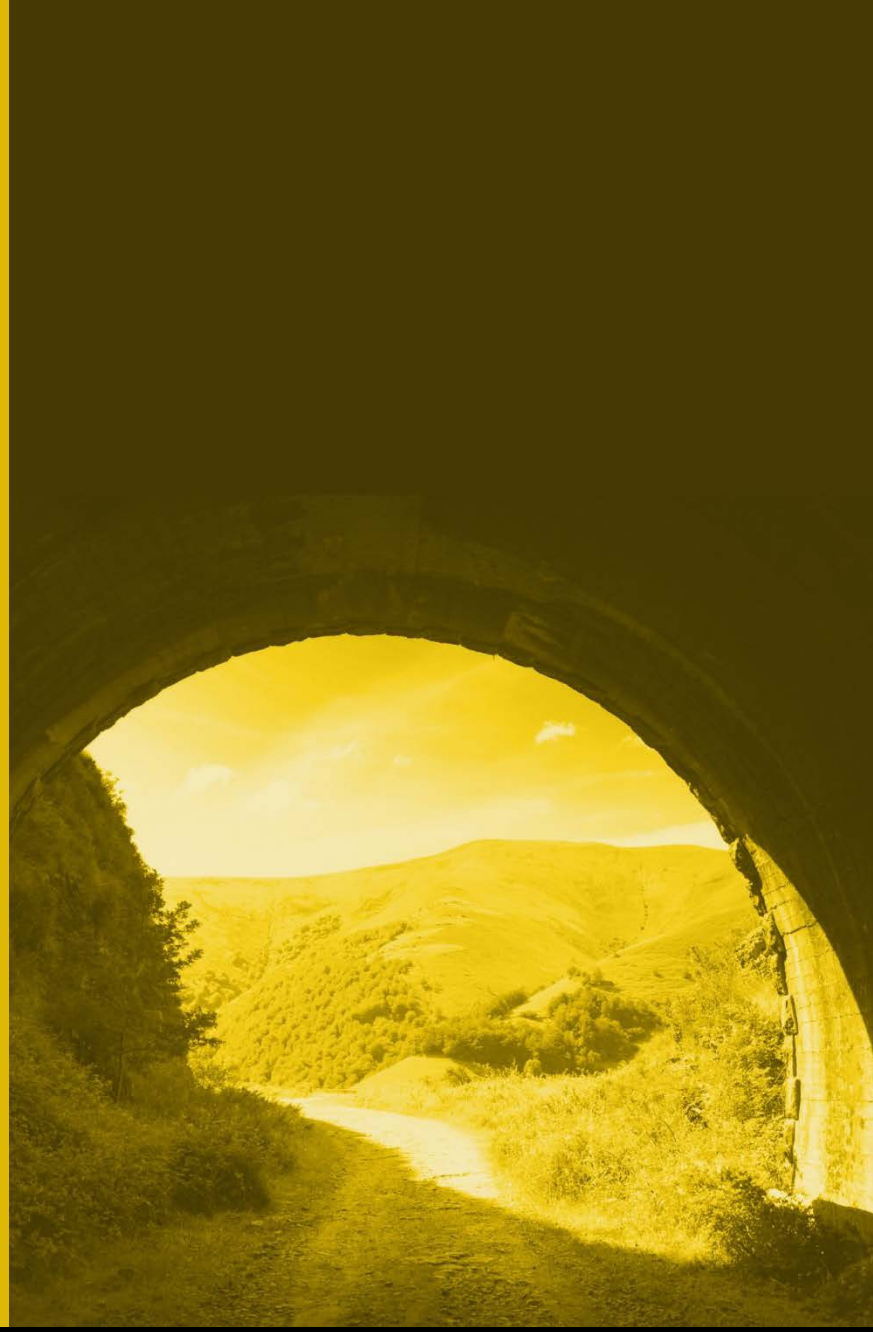
Software Reliance is Rapidly Expanding



Source: U.S. Air Force Scientific Advisory Board. *Sustaining Air Force Aging Aircraft into the 21st Century* (SAB-TR-11-01). U.S. Air Force, 2011.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software and Hardware Supply Chain Similarities and Differences



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0660

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Security Vulnerabilities are Increasing

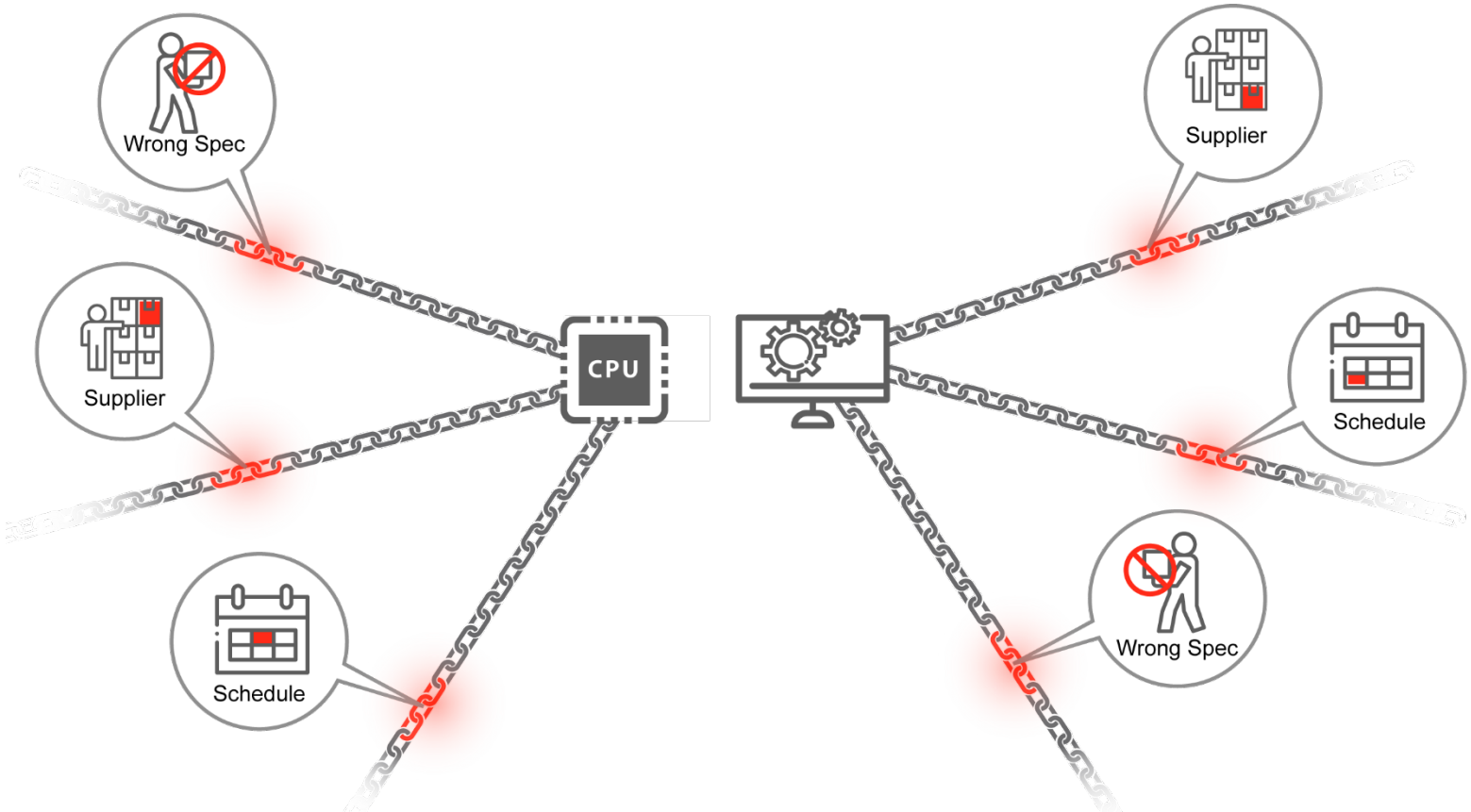
Definition: Security vulnerability is a weakness which allows an attacker to bypass security controls

Requires three elements:

- System susceptibility or flaw
  - Millions of lines of software code handling an ever increasing amount of functionality
  - Thousands of software vulnerabilities
  - Increased reliance on commercial and open source software
- Attacker access to the flaw
  - Increased connectivity linking systems to other systems and connecting to new types of devices (Internet of Things)
  - Increased system and device remote communication capability
- Attacker capability to exploit the flaw
  - Access to the same tools and techniques used to build software
  - Reverse engineering capabilities for commercial and open source
  - Malware and attack platforms and frameworks

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software and Hardware Supply Chains: *Shared Risks*



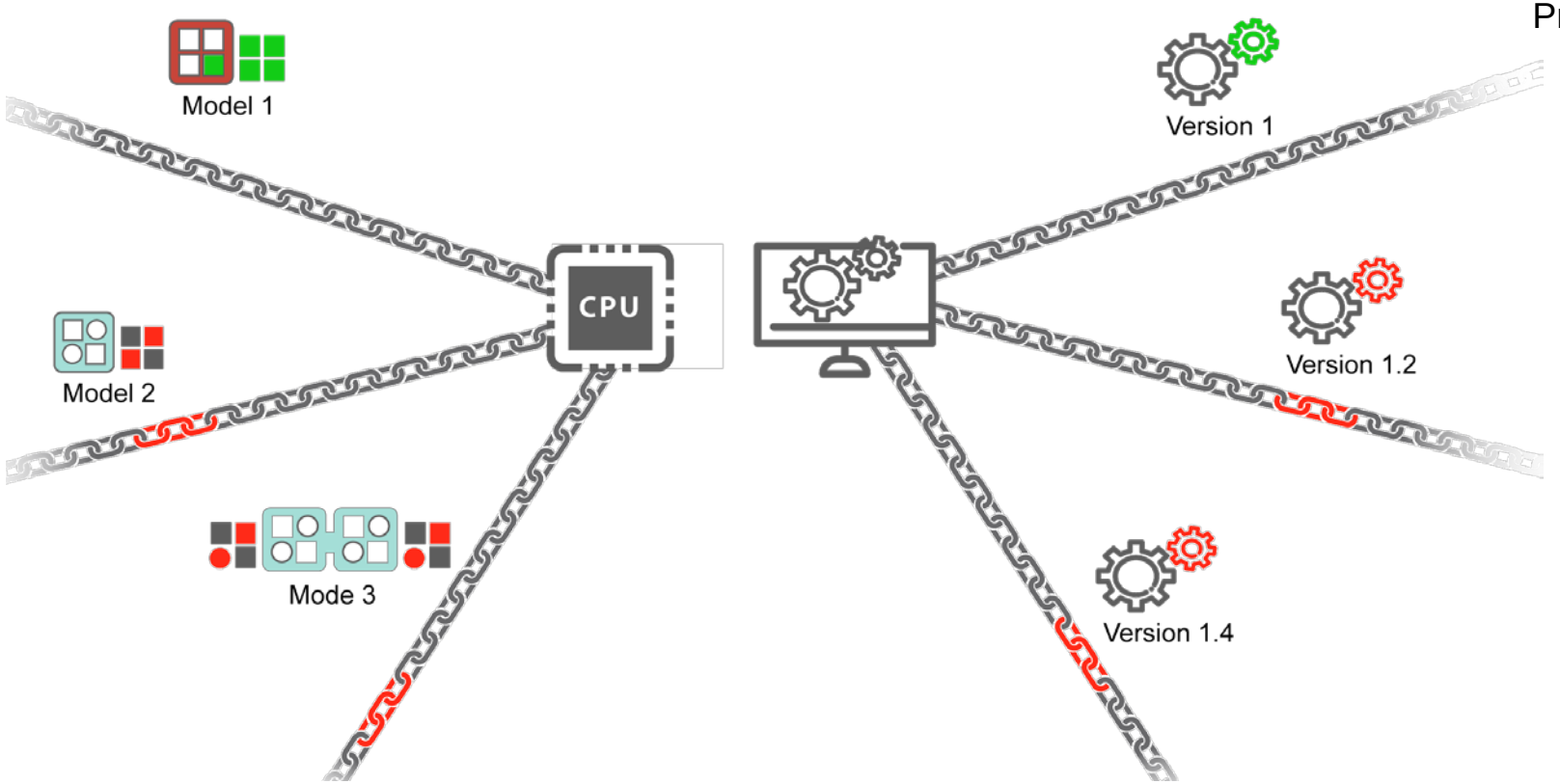
Hardware and software supply chains share a number of risks:

- Business risks associated with a supplier's operations
- Cost and schedule risks
- Risks associated with delivered items not meeting specifications

For shared risks, a software supply chain analysis framework can draw on experience with hardware supply chains.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software and Hardware Supply Chains: *Differences - 1*

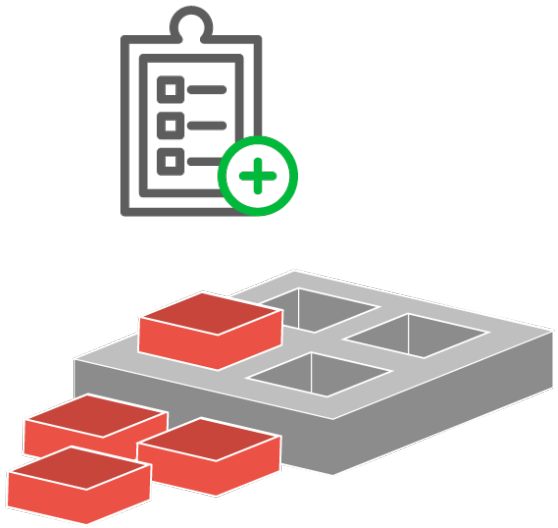


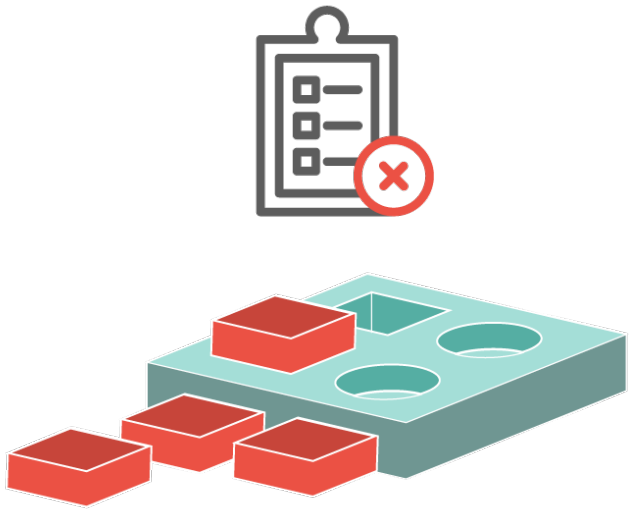
Product Features and Capabilities

- Hardware products comprise physical components
  - Not easily refactored after manufacturing
  - Difficult to add new capabilities that require changes to hardware
- Software products can evolve across multiple releases by
  - Adding new features and capabilities
  - Rewriting existing logic to support the new features and capabilities

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

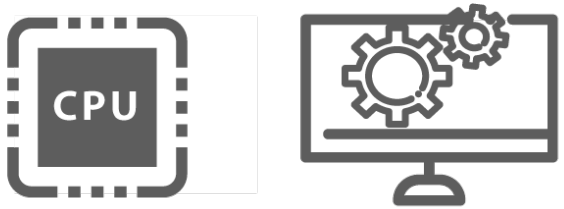
Software and Hardware Supply Chains: *Differences - 2*





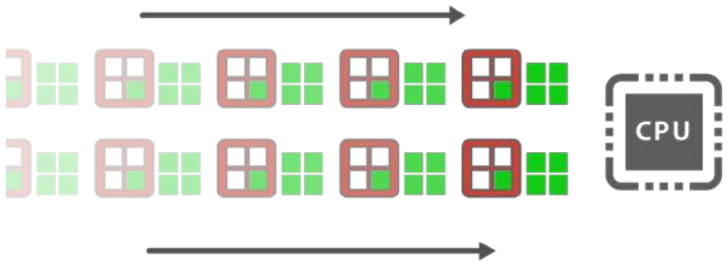
Product Verification

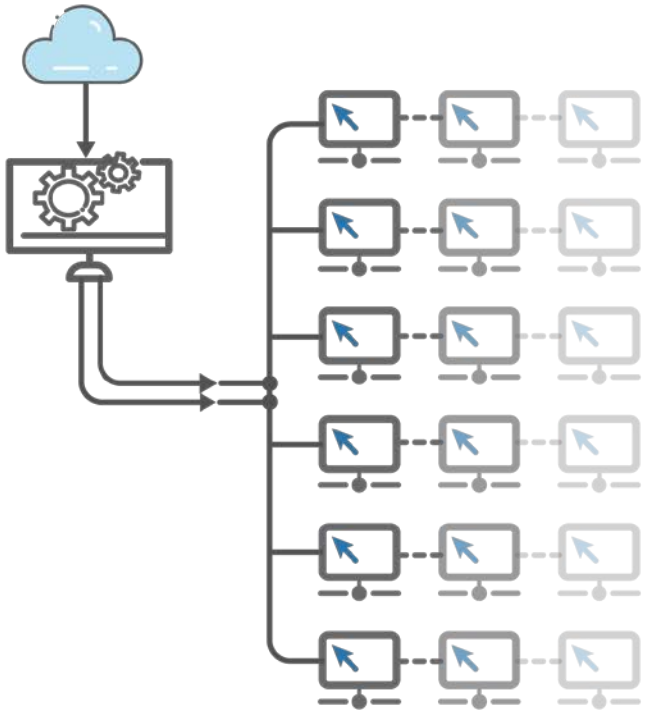
- Hardware specifications can be verified using visual inspection and closed loop testing on delivery in many instances.
- Software functionality cannot typically be verified on delivery.
  - A software component may exhibit undesired behavior when confronted with conditions not considered during development, raising a security concern.



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software and Hardware Supply Chains: *Differences - 3*





Product Distribution

- Hardware and integrated components involve multiple deliveries of the same item.
  - Supply chain integrity must be verified for each delivery.
- A software product is typically delivered as a single item that is then redistributed within an organization.
  - Issues of supply chain integrity apply to that one delivery.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software and Hardware Supply Chain Analysis: *Maturity*

Analysis of hardware supply chains

- Draws on decades of experience and data
- Has an established framework for research and analysis

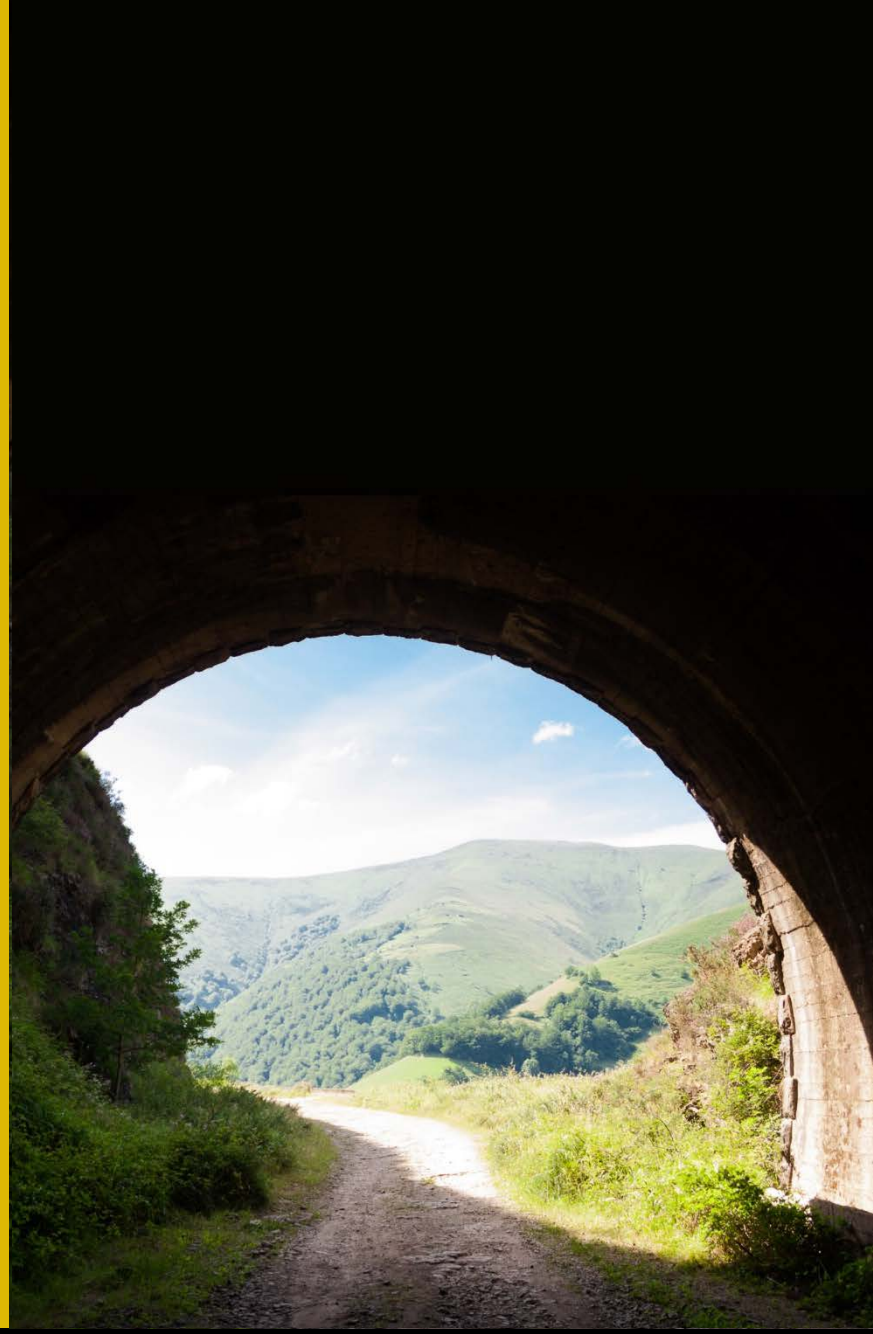
Analysis of software supply chains

- Does not have a comparable baseline of experience and data
- Is an evolving discipline

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquisition Strategy Drives the Structure of the Supply Chain

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0660

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquisition: Three Cases

Case 1 – acquisition organization has typical client role for new software

Acquisition Org.

Contractor Requirements

Case 2 – acquisition organization does requirements specification

Acquisition Org.

Requirements

Contractor

Case 3 – acquisition organization is purchasing COTS software

Acquisition Org.

COTS/GOTS

Open Source

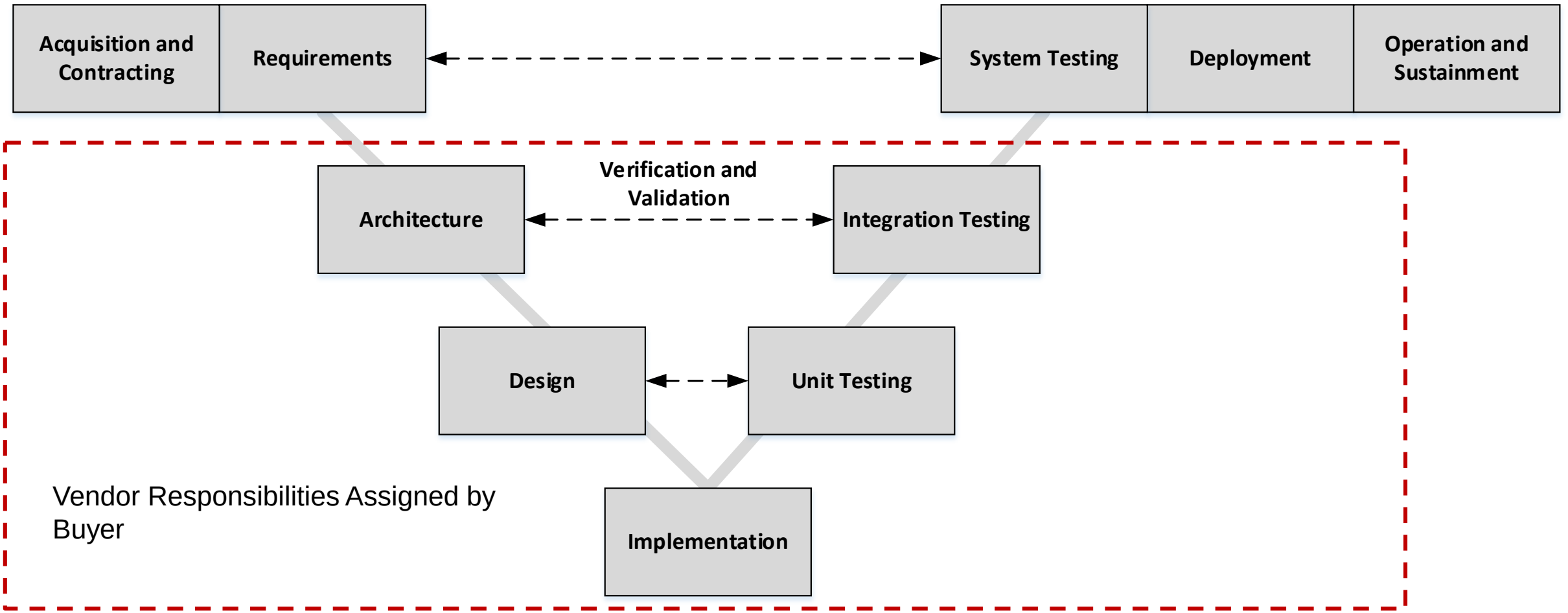
© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquisition Case 1 – Buyer to Vendor Relationships

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

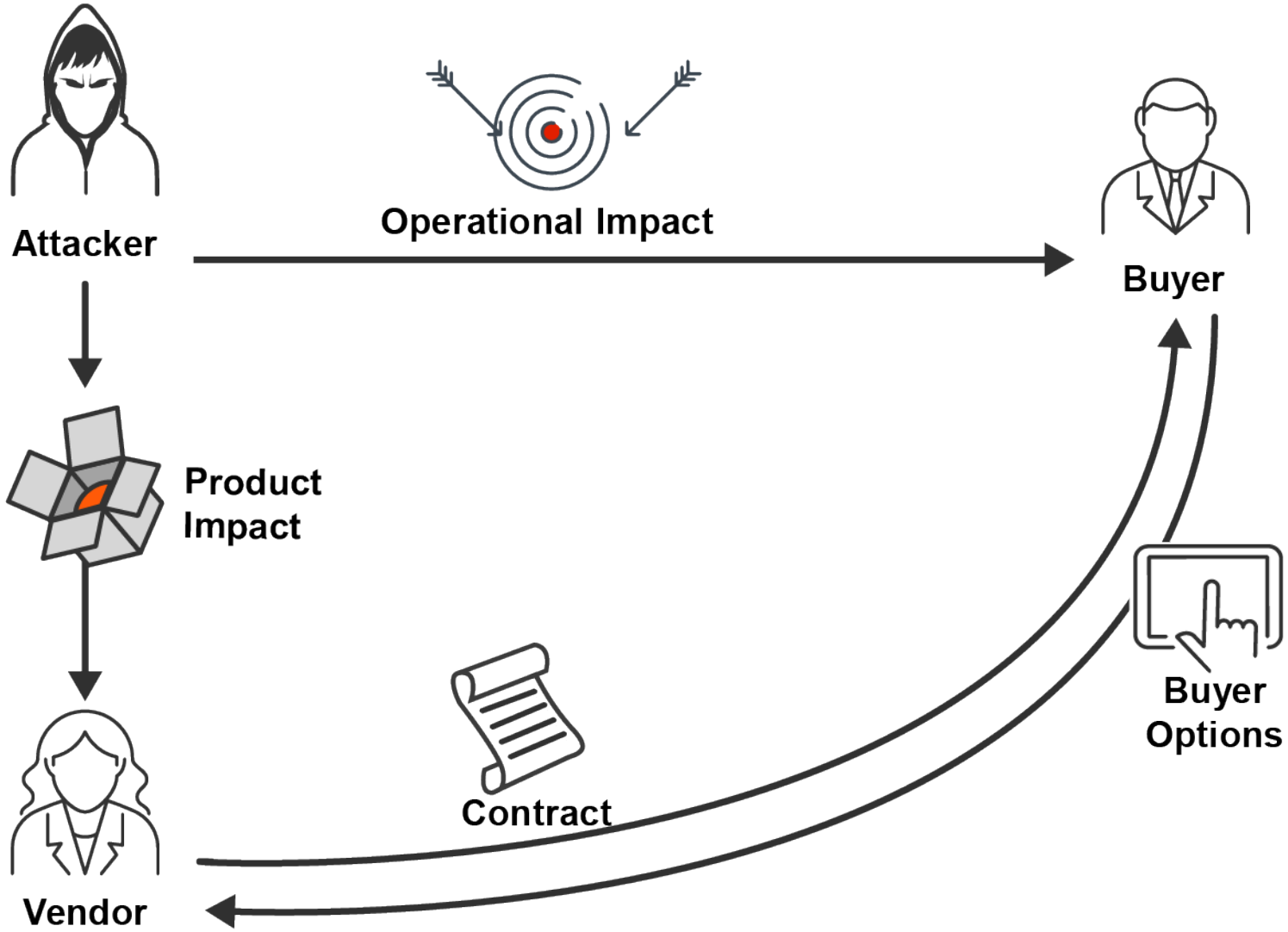
Acquisition Case 2 – Buyer View of the Acquisition

Buyer will focus on defining the requirements and the vendor will contract to deliver a product that meets those requirements.
The buyer will focus on confirming the delivered product meets requirements within the contracted cost and schedule.



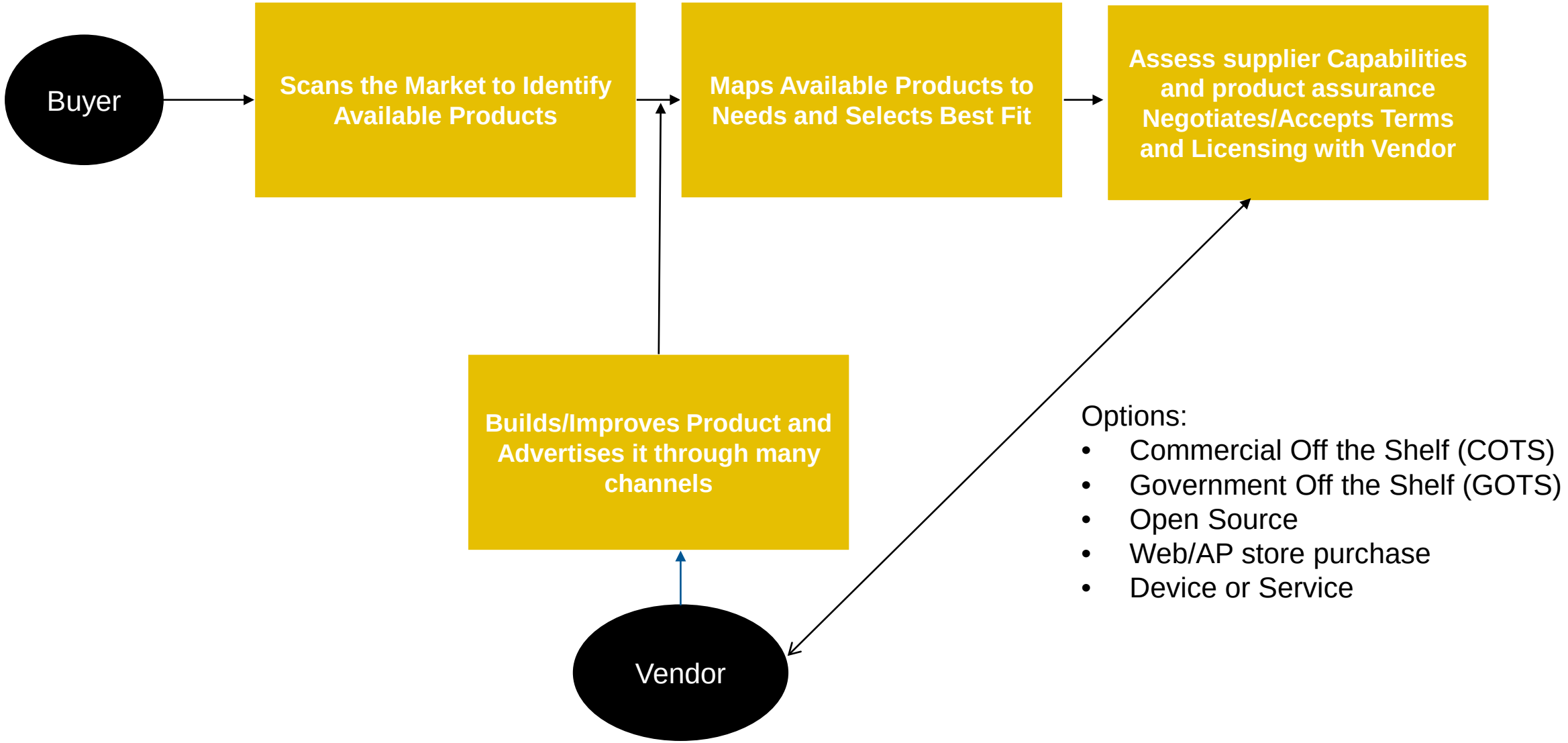
© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supply Chain Relationships for Case 1 and 2



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquisition Case 3 – Buyer View of the Relationship

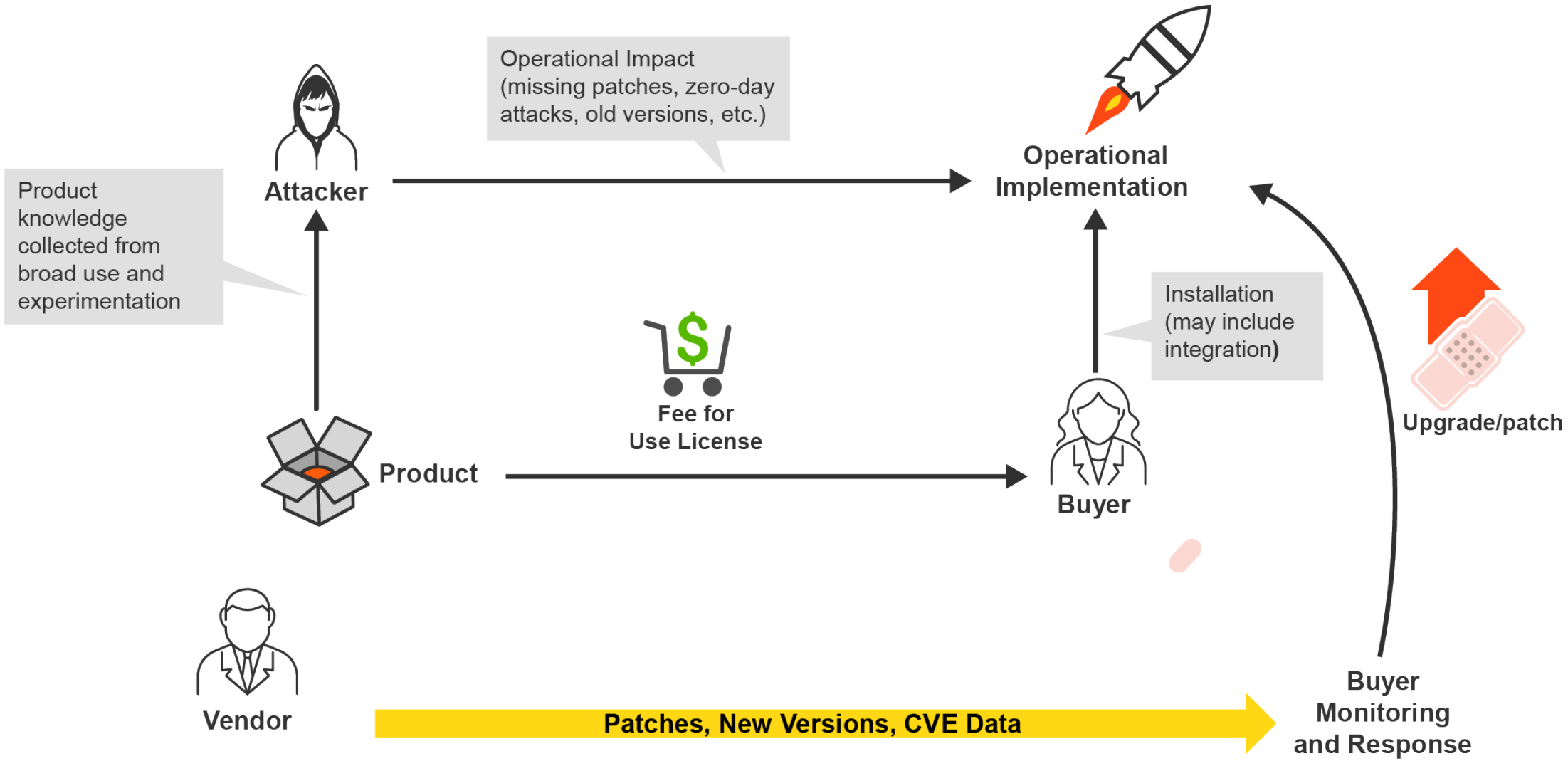


Options:

- Commercial Off the Shelf (COTS)
- Government Off the Shelf (GOTS)
- Open Source
- Web/AP store purchase
- Device or Service

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

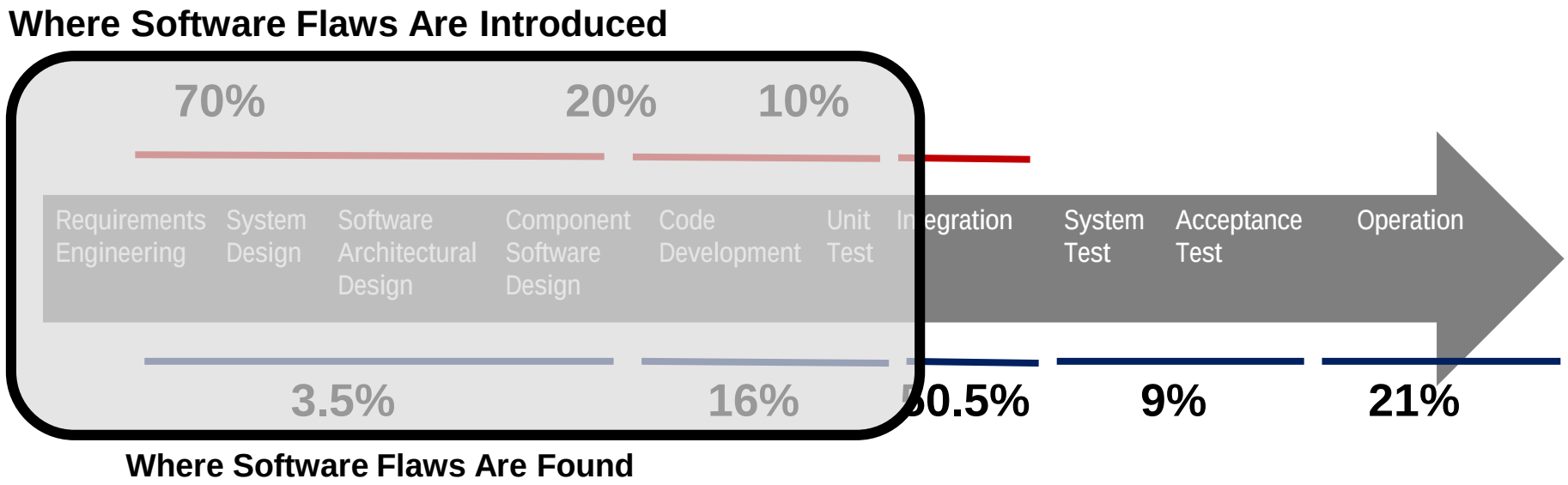
Supply Chain Relationships for Case 3



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquirer Visibility is Limited in All Cases

With supply chains, monitoring is indirect.

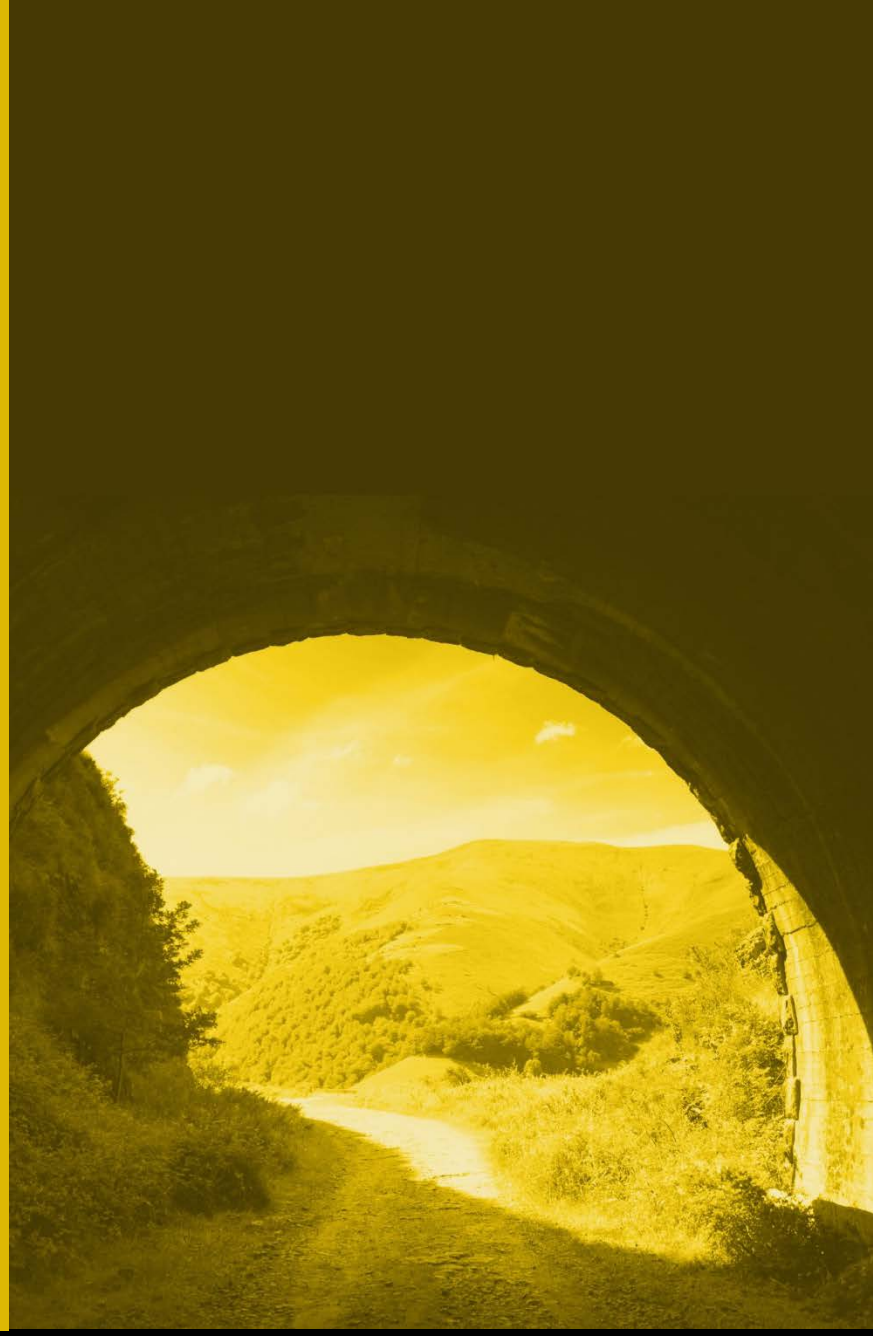


Improved focus on SCRM activities needed on the front end of the SDLC

Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supply Chain Assurance



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0660

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquisition: Three Cases

Case 1 – acquisition organization has typical client role for new software

Acquisition Org.

Contractor Requirements

Case 2 – acquisition organization does requirements specification

Acquisition Org.

Requirements

Contractor

Case 3 – acquisition organization is purchasing COTS software

Acquisition Org.

COTS/GOTS

Open Source

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Monitor SCRM Risk Factors

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

Evidence of Supplier Capability (S)	*Evidence of Product Security (P)*	*Evidence of Product Distribution (D)*	*Evidence of Product Operational Control (O)*
Supplier follows practices that reduce supply chain risks	Delivered or updated product is acceptably secure	Methods of transmitting the product to the purchaser guard again tampering	Product is used in a secure manner Fit-for-use

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

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

S – Evidence of Supplier Capability for Security

Supplier employees are educated in security engineering practices

- Documentation of training of each engineer, including when trained/retrained
- Revision dates for training materials
- Lists of acceptable credentials for instructors
- Names of instructors and their credentials

Supplier follows suitable security design practices

- Documented design guidelines
- Provides evidence that design and coding weaknesses that affect security have been addressed (Common Weakness Enumeration [CWE])
- Has analyzed attack patterns appropriate to the design such as those that are included in Common Attack Pattern Enumeration and Classification (CAPEC)

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

P – Evidence of Product Security

What product characteristics minimize opportunities to enter and change the product's security characteristics?

- Attack surface evaluation: Exploitable features have been identified and eliminated where possible
  - Access controls
  - Input/output channels
  - Attack enabling applications – email, Web
  - Targets
- Design and coding weaknesses associated with exploitable features have been identified and mitigated (CWE)
- Independent validation and verification of threat resistance

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

D – Evidence of Product Distribution

Is the product secure on delivery or are there steps the acquirer must take to make it secure?

Has the vendor provided ways so the product can be made effectively secure?

Are distribution mechanisms appropriate for maintaining product security? Does the vendor

- Require good security practices by their suppliers
- Assess the security of delivered products
- Address the additional risks associated with using the product in their context

Are patches and updates delivered in a timely and secure manner?

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O – Evidence of Product Operational Control

Who assumes responsibility for preserving product attack resistance with product deployment?

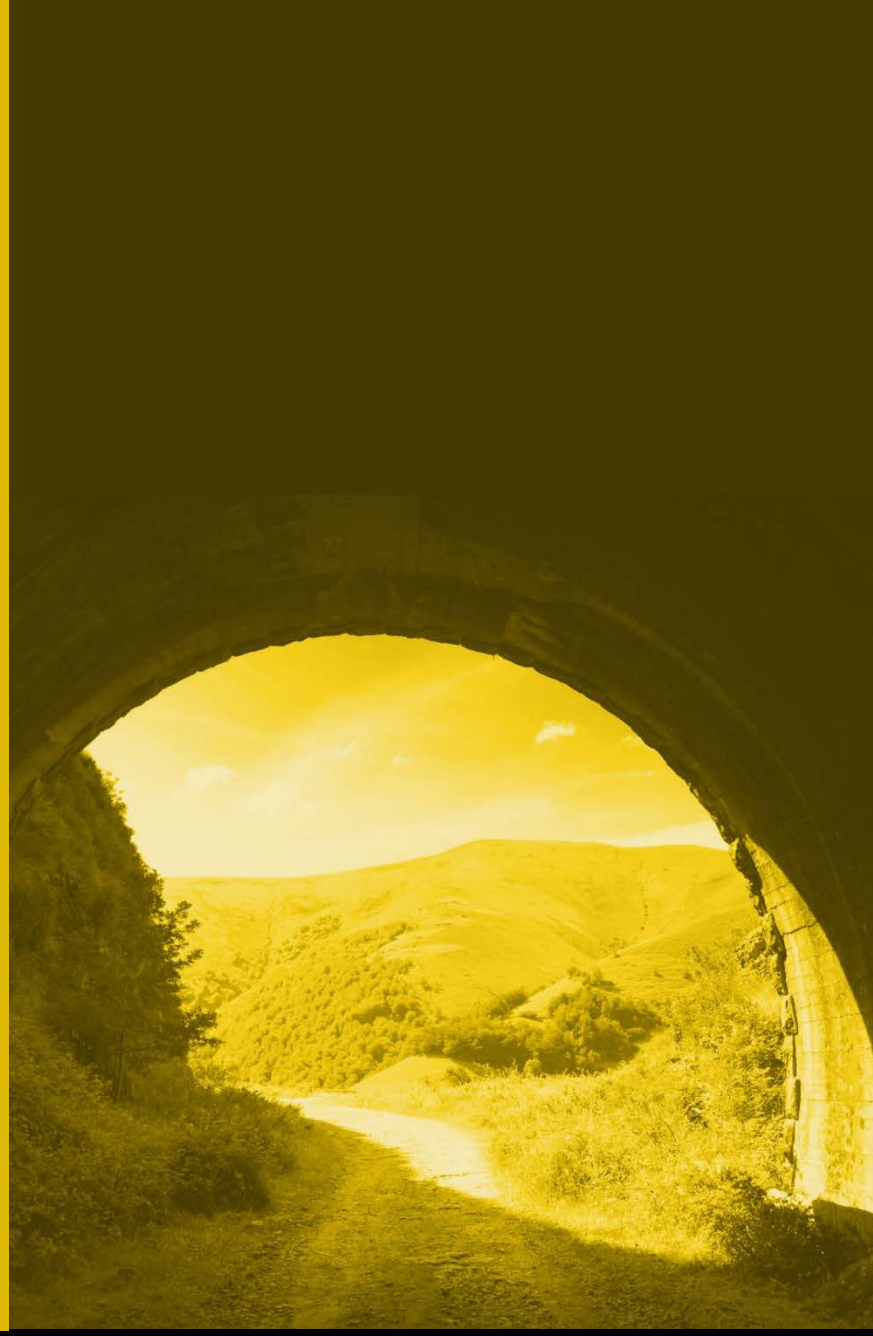
- Patching and version upgrades
- Expanded distribution of usage
- Expanded integration

Usage changes the attack surface and potential attacks for the product

- Change in feature usage or risks
- Are supplier risk mitigations adequate for desired usage?
- Effects of vendor upgrades/patches and local configuration changes
- Effects of integration into operations (system of systems)

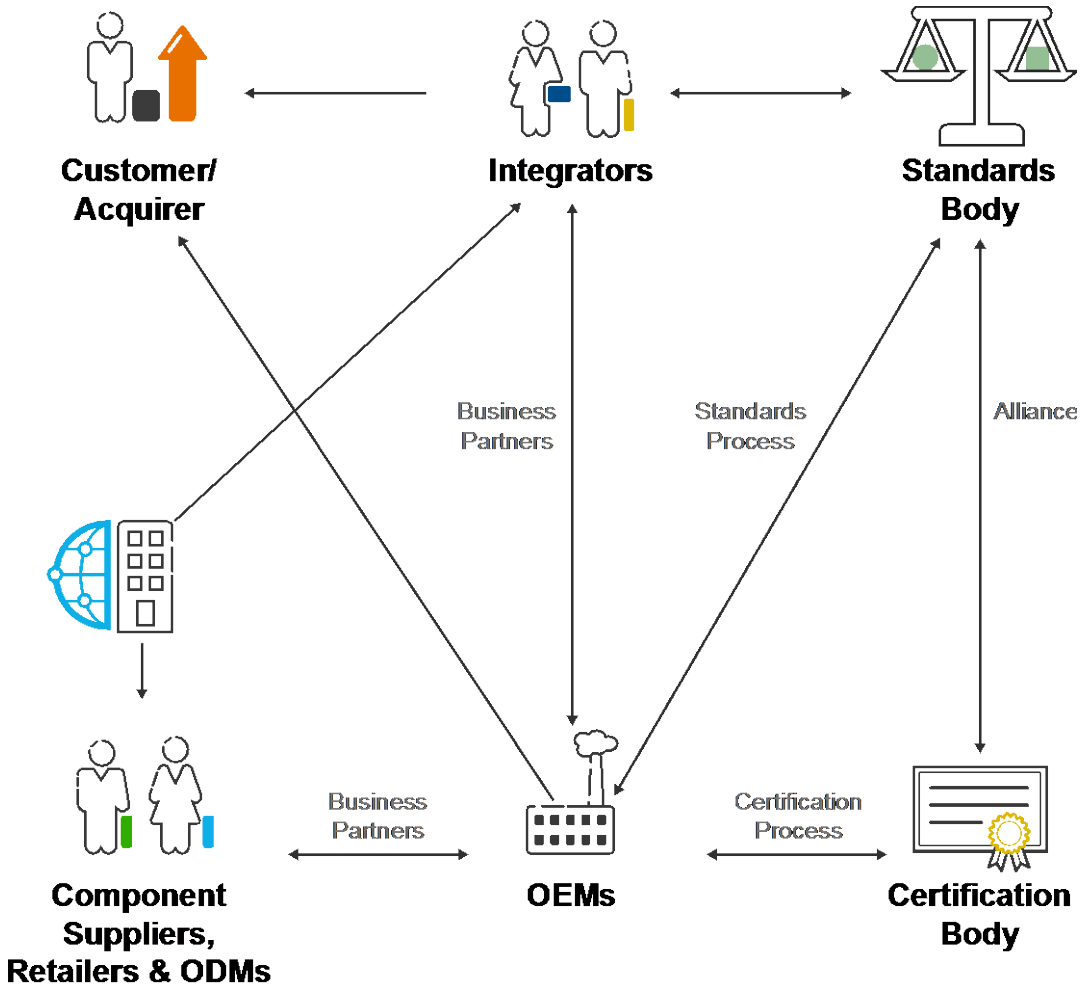
© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Product Supply Chain Risk Management (SCRM) Assurance (Evidence for Case 3)



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Demonstrating Assurance for Product SCRM Claims



http://www.opengroup.org/subjectareas/trusted-technology

Example: Open Group Open Trusted Technology Provider™ Standard (O-TTPS, an ISO standard) specifies a SCRM certification process.

- Identify SCRM claims (called requirements in O-TTPS) that should be met (product and supplier dependent).
  - Significant differences in processes and specific practices among suppliers
- Provide guidance for assessing each claim
- Identify and evaluate evidence that increases the assurance that a claim has been satisfied.

Certification assessment done by independent laboratory to control access to proprietary supplier product and development information

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O-TTPS Background

An Open Group task force developed a SCRM certification process which is now an ISO standard.

- https://ottps-cert.opengroup.org/ottps-standard
- https://ottps-cert.opengroup.org/docs/O-TTPS_Certification_Package_Document.doc

Focused on commercially available and widely applicable hardware and integrated products such as network routers. Did not address custom development.

Members of Open Group task force include commercial hardware, software, and integrated product suppliers; DoD; MITRE; Institute for Defense Analysis (IDA); and Software Engineering Institute (SEI).

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O-TTPS Evidence

The evidence sought should be artifacts that would normally exist if a supplier's practice satisfies the requirement.

- Threat analysis evidence - A list of known potential attacks, threat assessment against product architecture and design, vulnerability analysis during all phases, relevant threat analysis reports.
- Configuration management evidence - CM reports, build reports, CM tooling, CM artifacts, CM applications, tools, build tools, change control applications, reports produced from change boards.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O-TTPS SCRM Practices Certification Assessment

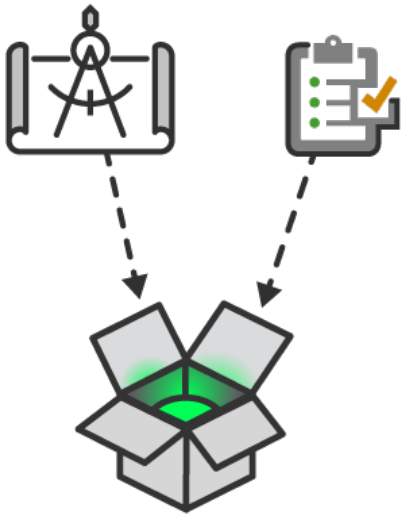
Practices reflect the supply chain experience of the Open Group member companies that participated in the development of the standard

A specific assessment considers an applicable subset of 24 practice areas.

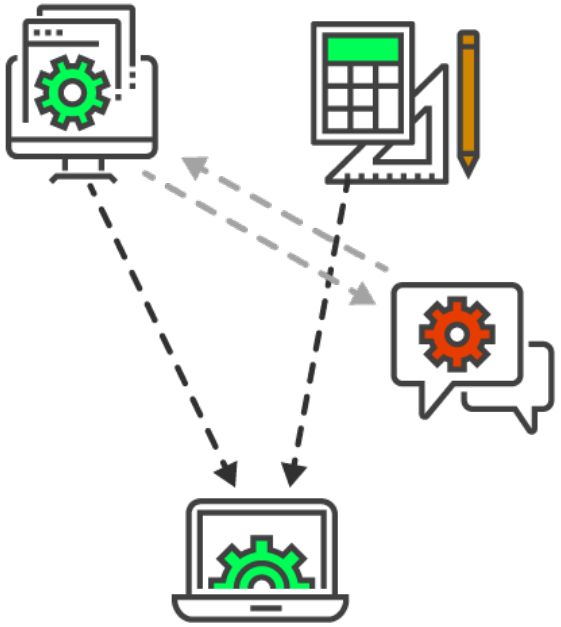
Practices to be evaluated depend on the products and the practices used by a supplier and are negotiated between supplier and the independent laboratory.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O-TTPS Claims



Threat Analysis Evidence



Configuration Management Evidence

Examples

- Product architecture and design shall be assessed against potential attacks to gain an understanding of the threat landscape.
- A documented formal process shall exist which defines the configuration management process and practices.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence of Supplier Capabilities and Product Security

Evidence for Quality Product Development	Supplier practices conform to best practice requirements and recommendations primarily associated with activities relating to the product development.
Evidence for Secure Development	Providers employ a secure engineering method when designing and developing their products. Software providers and suppliers often employ methods or processes with the objective of identifying, detecting, fixing, and mitigating defects and vulnerabilities that could be exploited, as well as verifying the security and resiliency of the finished products.
Evidence for Supply Chain Security	Suppliers manage their supply chains through the application of defined, monitored, and validated supply chain processes.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O-TTPS: Practice Areas - 1

Evidence of Supplier Software Development Capabilities

Configuration Management
Risk Management
Well-defined Engineering Processes and Practices
Software, Firmware, Hardware Design Process
Quality and Test Management
Product Sustainment Management

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Certification Configuration Management PD_CFM.01

A documented formal process shall exist which defines the configuration management process and practices.

Guidance: The configuration management process should include change management or separate process documentation should exist that covers change management.

Evidence:
Process: Configuration Management Process
Implementation: CM reports, build reports, CM tooling, CM artifacts, CM applications, tools, build tools, change control applications, reports produced from change boards

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Certification Configuration Management PD_CFM.05

Access to identified assets and artifacts and supporting systems shall be protected and secured.

Guidance: An overall access control policy shall describe the access control policy for each of the artifacts and assets under configuration management. This includes physical access control policies and logical access control policies. The Assessor shall check that the evidence demonstrates that the access control policy has been implemented.

Evidence: *Implementation:* Security audit reports, CM access control, problem tracking access control, build management access control, assembly management access control, access controls to physical artifacts, role-based or identity-based access controls, list of supporting systems

Related Requirements: All access control requirements

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O-TTPS: Practice Areas - 2

Evidence of Secure Development
Threat Analysis and Mitigation
Monitor and Assess the Impact of Changes in the Threat Landscape
Vulnerability Analysis and Response
Run-time Protection Techniques
Product Patching and Remediation
Secure Engineering Practices

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Certification: Threat Analysis and Mitigation SE_TAM.01

Product architecture and design shall be assessed against potential attacks to gain an understanding of the threat landscape.

Guidance: Determine whether the Organization has a process in place to assess their product architecture and design against the threat landscape and that they have implemented the process.

Evidence: *Process:* Product Design Process
Implementation: A list of known potential attacks, threat assessment against product architecture and design, vulnerability analysis during all phases, relevant threat analysis reports

Related Requirements: All risk management requirements
All Software/Firmware/Hardware Design Process requirements

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Certification: Threat Analysis and Mitigation SE_TAM.02

Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development

Guidance: Determine whether the Organization has a process in place to assess their product architecture and design against the threat landscape and that they have implemented the process.

Evidence: *Process:* Product Development Process
Implementation: Process and method artifacts

Related Requirements: Development process considers requirements during design.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Certification: Threat Analysis and Mitigation SE_TAM.03

Threat analysis shall be used as input to the creation of test plans and cases.

Guidance: The Assessor shall consider how threat analysis, from SE_TAM.01, is used as input to the creation of test plans and cases during the analysis of requirement PD_QAT.01. Quality and test product plan includes quality metrics and acceptance criteria.

Evidence: *Process:* Product Test Process

Related Requirements: Testing and quality assurance activities are conducted according to the plan.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O-TTPS: Practice Areas - 3

Evidence of Supply Chain Security

Open Source Handling	Trusted Technology Components
Physical Security	Secure Transmission and Handling
Malware Detection	Counterfeit Mitigation
Access Controls	Business Partner Security
Risk Management	Information System Security
Supply Chain Security Training	Employee and Supplier Security and Integrity

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Limited Applicability of O-TTPS

Commercial products

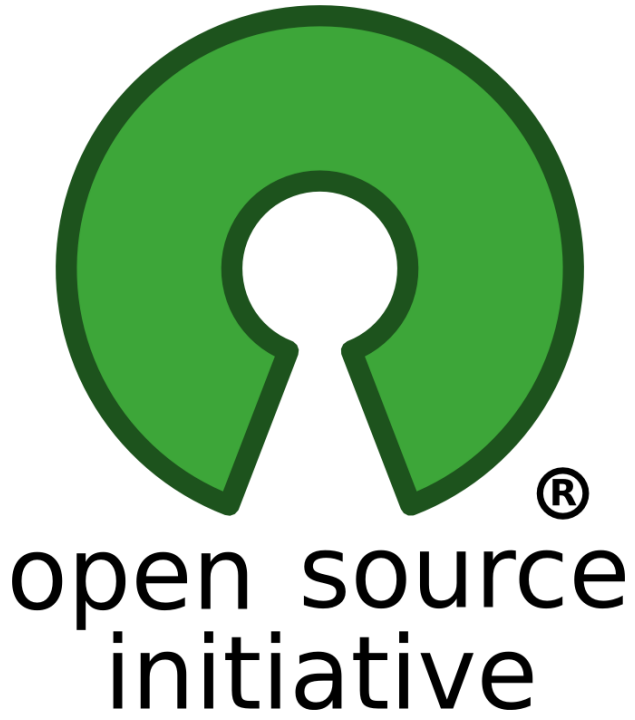
- fit-for-use: Has the product been designed to manage the risks in the proposed operational environment?

Limited SCRM associated with

- consumer-based technology: cell phones
- leading-edge technology: internet of things
- open source software

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

What about open source? Apply similar practices but with different resources



Source: http://opensource.org/

46 million vulnerable open source components downloaded annually

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence of Supplier Capability: Open Source Products

O-TPPS requirements are often impossible to verify for open source products.

Example: Heartbleed vulnerability in OpenSSL, a widely used open source implementation of the secure socket layer protocol used for securing web communications

- Heartbleed vulnerability potentially exposed memory data to unauthorized users which might include passwords, user identification information, and other confidential information.
- At time of announcement in 2014, there did not appear to be any tools that would have discovered the vulnerability.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

OpenSSL Example

The vulnerability occurred because the input to the OpenSSL *assert* function was not validated (one of the Top 25 Most Dangerous Software Vulnerabilities).

Open source software such as OpenSSL often addresses aspects of some of the O-TTPS claims, such as configuration management, while other areas such as design practices are delegated to individual developers.

The O-TTPS assumption is that the OpenSSL vulnerability would be much less likely to occur with suppliers whose practices satisfy the O-TTPS threat analysis, design, and testing requirements.

Demonstrating the assurance of security claims often falls to the acquirer of open source software.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Open Source: Equifax

The attack community appears to closely follow vulnerabilities in Open Source software.

The 2017 attack on Equifax exploited a vulnerability in Apache Struts.

- The supplier released a patch to fix the vulnerability on March 6, 2017.
- Three days later, the bug was already under mass attack by hackers who were exploiting the flaw to install rogue applications on Web servers. https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/
- Equifax has said that the breach on their server occurred in mid-May.

Patches for open source and widely-used COTS software should be rapidly applied.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

O-TTPS: Open Source

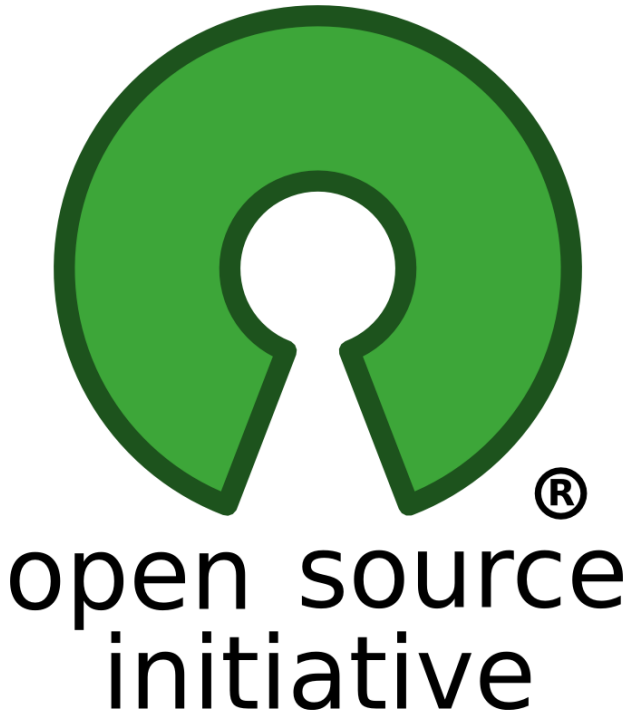
For such sourced components, responsibilities for ongoing support and patching shall be clearly understood.

In the management of Open Source assets and artifacts, components sourced shall be identified as derived from well-understood component lineage.

In the management of Open Source assets and artifacts, components sourced shall be subject to well-defined acceptance procedures that include asset and artifact security and integrity before their use within a product.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

What about open source? Apply similar practices but with different resources

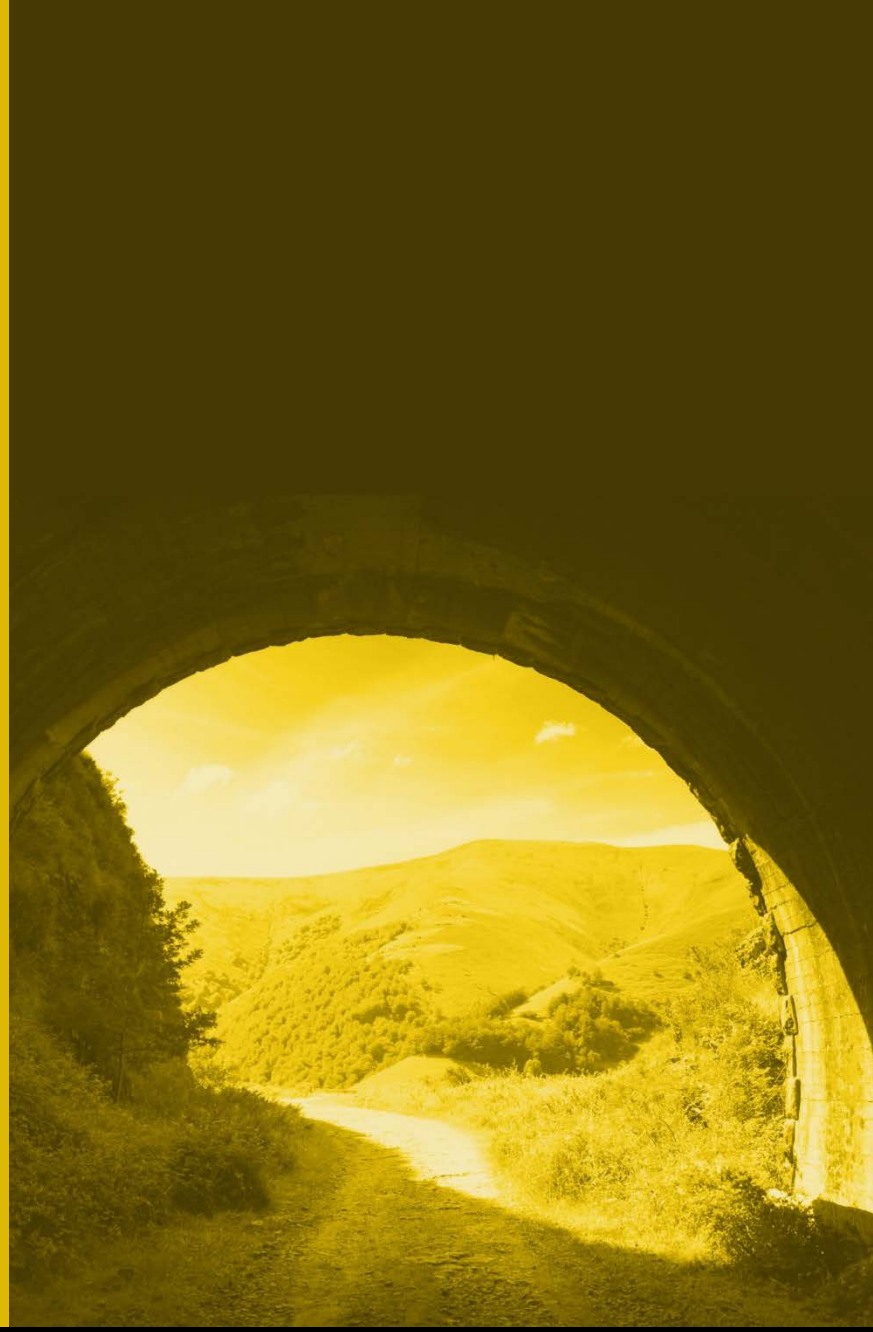


Source: http://opensource.org/

- Establish an internal resource to monitor open source components
- Establish a process for tracking open source vulnerabilities
- Monitor and restrict open source components that can be used
- Establish an internal open source component distribution process to keep internal versions current
- Maintain a registry of where open source components are used
- Institute an update policy to remediate discovered and patched vulnerabilities

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Requirements and Assurance (Case 2 & 3)



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Software Requirements

Commercial software typically provides customization and extensibility capabilities so that the product has wider applicability.

Such features provide the capability to recover from faults and to adapt to changes in operational requirements and security threats.

Attackers can use the same capabilities to change a system's behavior. Attacks often exploit specific features. Mitigations need to be in place to monitor system behavior to ensure the software functions as intended.

- Consider functional security risks as part of requirement analysis
- Increase acquisition review to ensure the product or system functions only as intended

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Market Demand for Customization and Extensibility

Customization: adapt functionality for desired usage

- database management software – select product services and specify data
- often implemented via configuration management
- run-time configurations: fault management, load management

Extensibility: add functionality

- web browser
- cell phones
- control systems – traffic lights, assembly lines, power generation,
- database management systems: user-programmed services

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquirers' Tug of War: Features Vs. Security

Web page:

Data & display instructions + Application code to process data

Web Site

Using Google's Gmail is equivalent to installing a software application

Extensibility

Browser functionality can be extended by adding the capability to execute programs such as those written in JavaScript (Google's Gmail).

Browser could be compromised by executing a page with embedded malware or by vulnerabilities in the downloaded code.

Smart phones

Industrial control systems

Web browsers & applications

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Customization and Extensibility Affect SCRM

Who does the customization, develops the additional functionality, and integrates the additional functionality?

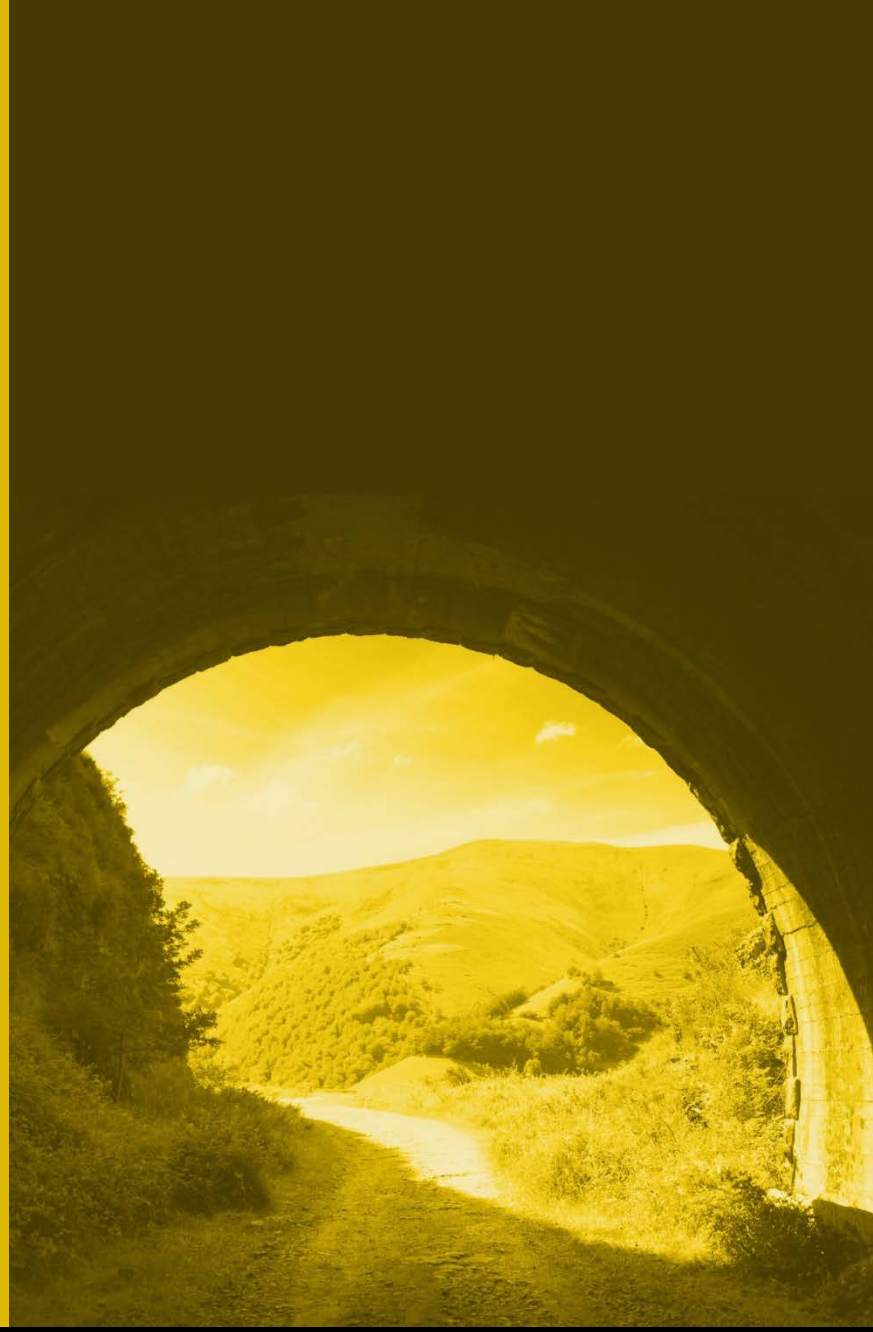
- end-user
- in-house
- externally developed – contracted, shared, commercial

SCRM requirements depend on where in acquisition lifecycle extensibility and customization are done, which should be specified by the acquisition.

- during development
- at product start-up – configuration files, control systems
- run-time: web browser, cell phone, real-time fault management, machine learning systems

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Custom System SCRM Assurance (Case 1 & 2)



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquisition: Three Cases

Case 1 – acquisition organization has typical client role for new software

Acquisition Org.

Contractor Requirements

Case 2 – acquisition organization does requirements specification

Acquisition Org.

Requirements

Contractor

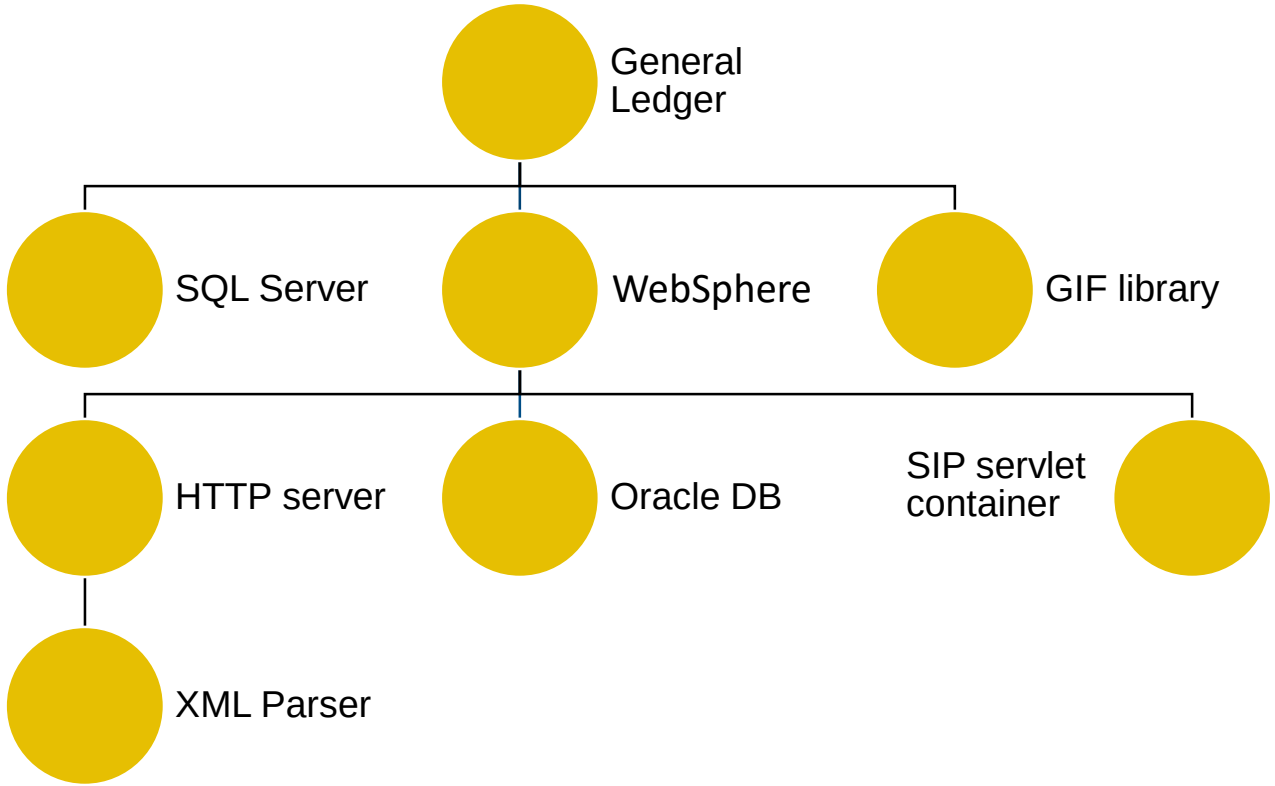
Case 3 – acquisition organization is purchasing COTS software

Acquisition Org.

COTS/GOTS
Open Source

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Challenges from Products to Systems



Integrating independently developed components with limited visibility into the actual code

Inconsistencies in security assumptions among components

Component behavior is dynamic over time and each component is supported and updated separately

- extensibility and customization
- product upgrades
- multiple components compound threat analysis and mitigations

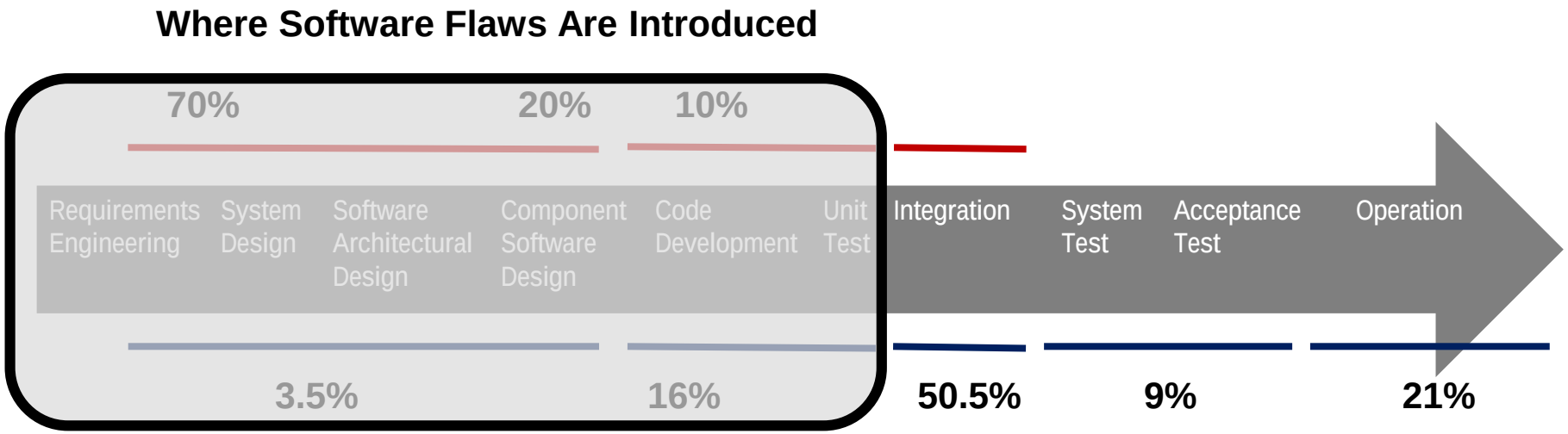
SCRM must include the integrated system as well as each separate component

The system may also include critical components considered to be part of the acquiring organization's infrastructure which are typically supported by another area of the organization

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

System Integration: Limited Visibility

Faults account for 30–50% of total software project costs.



An integrator has limited visibility on where faults could be created unless they are actively evaluating each selected product

Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Mitigate Inconsistencies Among Security Assumptions

Security assumptions for commercial products

- internal authentication and authorization functions
- input verification
- trust assumptions that guided design: for example, trust associated with internal network and external data sources
- fault management and recovery

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Differences in Product and System SCRM

The O-TTPS certification is designed for products rather than for system development

Practice areas such as Configuration Management and Threat Analysis and Mitigation apply to both types of development but the scope is quite different.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Threat Analysis and Mitigation – Product Vs. Systems

Product Development

Relatively Static Knowledge Specific to a Product

Threat analysis can be incrementally developed over the life of a product.

Functionality is typically static within a product version

Product developer can

- use history of weaknesses to improve specific development practices and training
- take advantage of historical knowledge of a typically small and static set of suppliers
- maintain integration expertise for a relatively static set of externally developed components.

Integrated System

General Knowledge Applicable Across Multiple Systems

Threat analysis must be developed for each integrated system

Integrator

- develops mitigation techniques for multiple sets of externally developed components
- is knowledgeable of risks and mitigations associated with required functionality such as those for extensibility and customization.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

System Integrators Development Capabilities: Top-level Objectives

Applied across the full development lifecycle

- design analysis
- security testing

Maintains expertise in system risks and available tools to support efficiencies

- up-to-date attack and threat knowledge
- knowledge and use of appropriate standards
- continuous training

Example practice: establishes effective monitoring through the consistent and effective use of metrics

- establish security checkpoints and milestones at various points in the development lifecycle
- require security signoffs at various points in development

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

BSIMM Scores for Top 10 Firms

Governance

Intelligence

Development

Deployment

System development requires general purpose software development capabilities

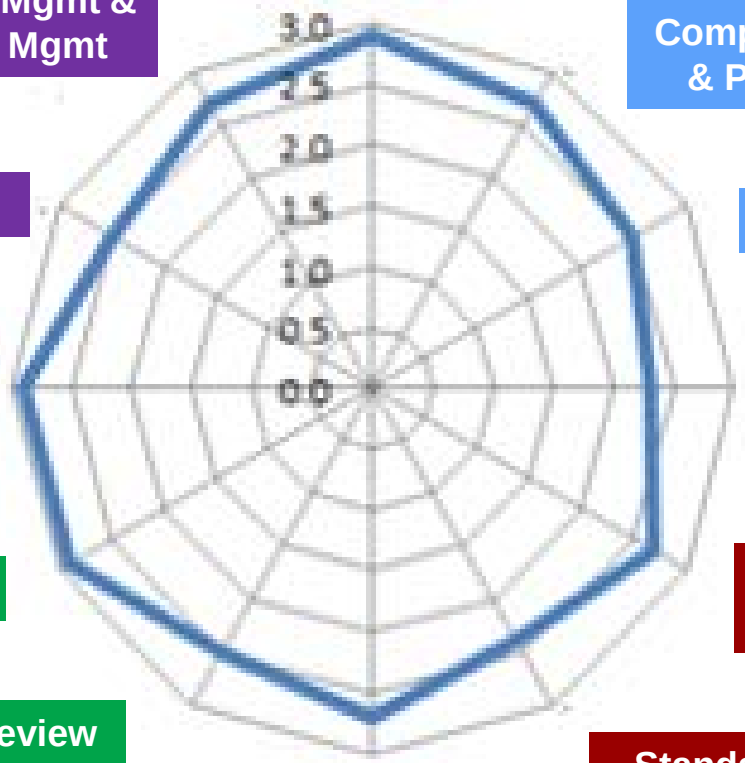
Strategy & Metrics

Configuration Mgmt & Vulnerability Mgmt

Compliance & Policy

Software Environment

Training



Penetration Testing

Attack Models

Security Testing

Security Features and Designs

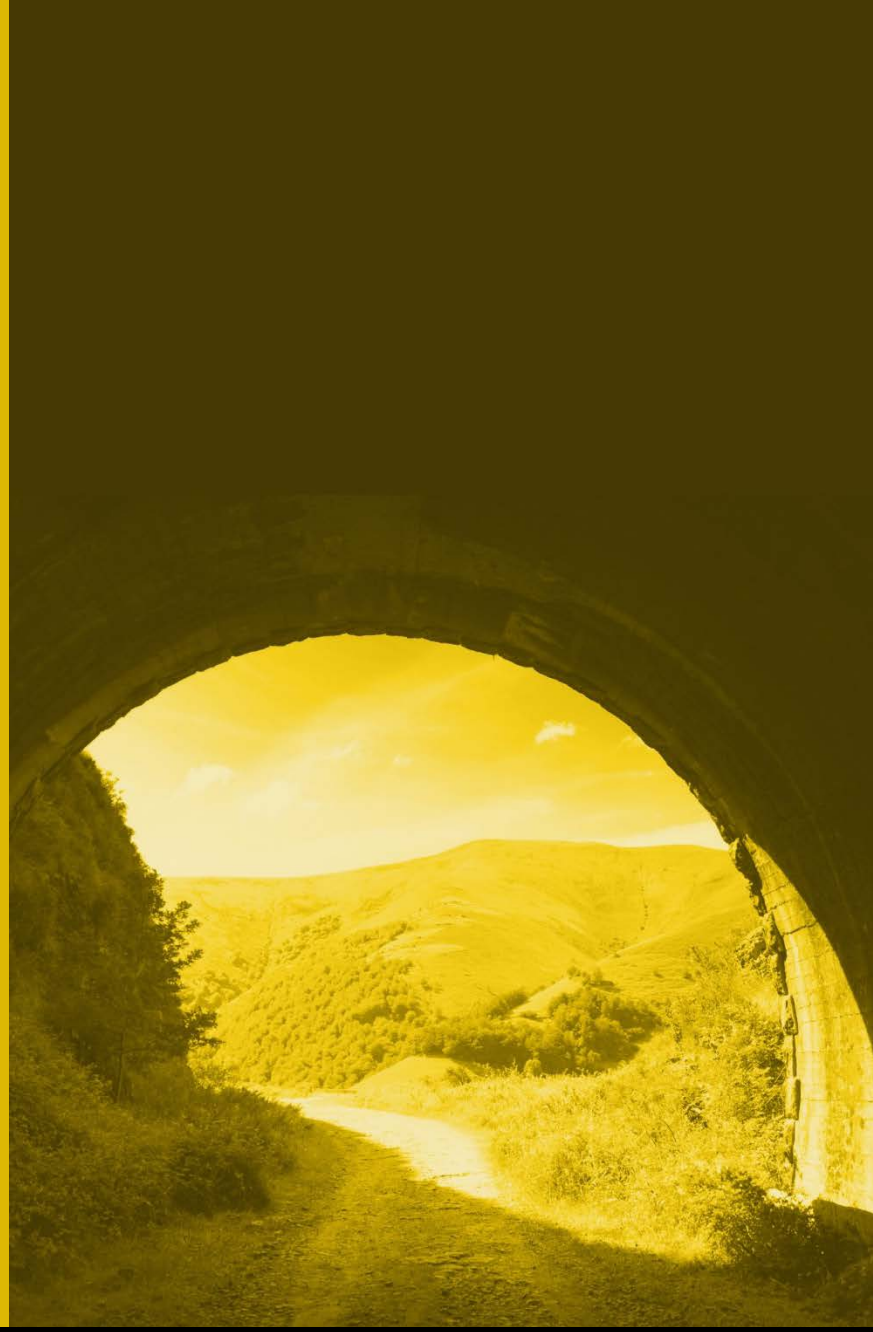
Code Review

Standards & Requirements

Architecture Analysis

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Supply Chain Risk Management (SCRM) Summary



© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0660

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

SCRM Strategies Vary Based on the Type of Acquisition

Case 1 – acquisition organization has typical client role for new software

Acquisition Org.

Contractor Requirements

Case 2 – acquisition organization does requirements specification

Acquisition Org.

Requirements

Contractor

Case 3 – acquisition organization is purchasing COTS software

Acquisition Org.

COTS/GOTS

Open Source

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Risk in the Software Supply Chain

Evaluate software supply chain risk in the larger context of

- Vendor supplier risk
- Product risk
- Distribution risk
- Operational risk

Risks to a business process or mission thread can come through the software supply chain

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Acquisition Assurance

Acquirers should use supply chain risk management to:

- identify potential security risks associated with requirements
- support the creation of supplier selection criteria
- include security risk management expertise to assist in source selections
- understand the security impact of choices

For products, we have described how a vendor can use certifications and the practices required within these to establish a level of product assurance to demonstrate their capabilities in addressing supply chain risk management. An acquirer can use certification results to influence choices among production options.

© 2017 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.