

# Supply-Chain Risk Management Framework

Carol Woody

March 2010



**Software Engineering Institute**

**Carnegie Mellon**

© 2010 Carnegie Mellon University

# Scope of SEI Work

## Context

Significantly reduce the risk (any where in the supply chain) that an unauthorized party can change the behavior of software in a way that adversely affects the security properties of the deployed product

## Proposed Approach

- Identify the supply chain and the controls in place to monitor software
- Document supply chain security risks that need to be mitigated, possible mitigation actions, and potential evidence needed to determine whether the mitigations are being implemented effectively
- Build an acquisition and deployment plan to address critical risks



# System Acquisition Security Process Lifecycle

Step	Sample Supply Chain Security Risk Management Activities
Initiation	Initial risk assessment Develop Request for Proposal Plans for monitoring supplier Select suppliers
Development	Manage acquisition Maintain awareness of supplier security management
Deployment	Assess delivered products Configure/Integrate User guidance
Operations/Maintenance	Incident handling Review operational readiness Monitor component/supplier
Disposal	Evaluate disposal risks Mitigate risks during disposal



# How do we know supply chain risk has been addressed?

The supply chain is well understood and documented.

Available evidence indicates that identified risks have been adequately reduced.

For gaps in evidence, the impact of associated supply-chain risks have been evaluated.



# Areas of Supply Chain Risk Review

Evaluate a supplier's security commitment

Evaluate a product's threat resistance

- Evaluate impact of supply-chain risks on product deployment and operations

Evaluate product delivery mechanisms

- License control
- Chain of custody

Maintain attack resistance during use



# Evaluate a Supplier's Security Commitment

How do we know that a vendor is seriously considering security?

- Organizational policies and practices support security
  - Employee education in security engineering practices
- Good processes are used to support development of secure products
- Good practices are applied for responding to security problems
- Good practices and policies are used for evaluating the security capabilities of its suppliers



# Supplier Security Commitment Evidence

Supplier employees are educated as to security engineering practices

- Documentation for each engineer of training and 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)



# Evaluate a Product's Threat Resistance

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

- Exploitable features have been identified and eliminated where possible (attack surface)
  - 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

Supplier and acquirer responsibilities are clearly assigned?

- Development and Integration
- Deployment and Operations



# Maintain Attack Resistance

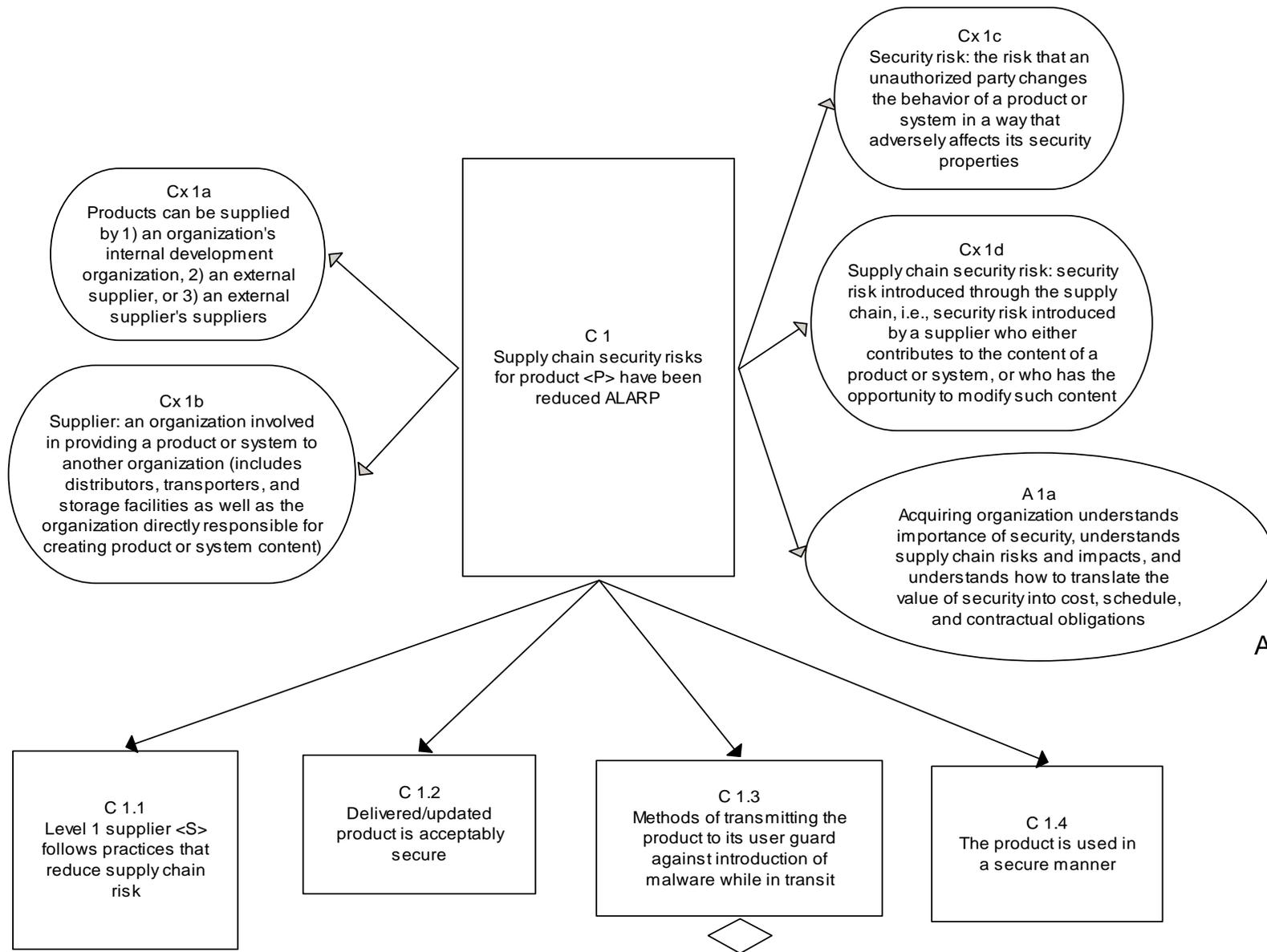
Who assumes responsibility for preserving product attack resistance with product deployment?

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

How are usage changes identified and addressed?

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





Created with ASCE Educational licence - valid for non-commercial teaching and research purposes only



# Findings from Pilot - 1

No widely accepted standards specifying what constitutes “proper” training software engineers

- developers using code generators need specifics on how to produce secure products within the limitations of these tools

Insight into vendor handling of subcontractors will require careful consideration

- subcontractors will reveal security issues to the government but not to the contracting vendor (potential competitor on future bids)

Security considerations are not primary in acquisition decisions for:

- Choice of vendor proposed solutions (except for specific security features such as PKI, certificates, encryption, etc.)
- Choice of program language
- Life cycle development practices



# Findings from Pilot - 2

Products must be “well behaved” but

- no monitoring for specific threats or vulnerabilities
- no formal acceptance criteria for COTS or code generated from COTS frameworks
- review is performed by Quality Control personnel with limited security expertise

Focus on software engineering principles

- isolation of interfaces to minimize data visibility and maximize information hiding
- isolation of performance-sensitive software
- encapsulation of COTS components

Operational product monitoring

- relying on logging which may be turned off for performance needs



# Summary

Current acquisition security focus is on infrastructure components and not applications

Lack of appropriate contractual requirements makes it difficult for a program office to determine if key supply chain security risk management practices are being followed

Acquisition practices are currently weak in assuring that deployment practices and operational practices are adequate to maintain security against supply chain security risks



# Next Steps

Developing a supply chain risk assessment

- Easy to learn and use
- Planning for future self-assessment

Seeking government agencies and contractors interested in piloting the assessment – see Bob Ellison to volunteer



## 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.**

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.



# Back-up Slides



# Definitions

## **Supplier:**

an organization involved in providing a product or system to another organization (includes distributors, transporters, and storage facilities as well as the organization directly responsible for creating product or system content)

## **Supply chain (SC):**

all suppliers, direct or indirect, having opportunity to modify the content of a product or system (includes those contributing to the content)

## **Supply chain security risk:**

security risk introduced by a supplier who either contributes to the content of a product or system, or who has the opportunity to modify such content



# Supply Chain Security Risk - 1

Apply to the acquiring organizations and their suppliers

- 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

Recognize that supply chain risks are accumulated

- Subcontractor/COTS-product supply chain risk is inherited by those that use that software, tool, system, etc.



# Supply Chain Security Risks - 2

Incorporate supply chain security risks considerations into the existing acquisition processes

- What aspects of supply chain security risks have been considered?
- For many acquisitions, a significant portion of supply chain security risk management has to be delegated to the prime contractor.
  - What aspects of supply-chain risk management have been assigned to the prime contractor?
  - Does this include requirements for managing supply-chain risks for sub-contractors?



# Contact Information

***Carol Woody***

(412) 268-9137

[cwoody@cert.org](mailto:cwoody@cert.org)

***Robert Ellison***

(412) 268-7705

[rellison@sei.cmu.edu](mailto:rellison@sei.cmu.edu)

***Web Resources (CERT/SEI)***

<http://www.cert.org/>

<http://www.sei.cmu.edu/>

