# Supply-Chain Risk Management Framework

Carol Woody, Ph.D.

December 9, 2010

# Scope of SEI Case Study

## Challenge

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

## Analysis Approach

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

# Areas of Supply Chain Risk Review

Evaluate supplier security commitment

Evaluate a product's threat resistance

Evaluate how the supplier maintains threat resistance during use

# Evaluate Supplier Security Commitment

Does the supplier follow suitable security design practices?

- Documented design guidelines
- Evidence that design and coding weaknesses have been addressed (Common Weakness Enumeration (CWE))
- Evidence of attack pattern analysis (Common Attack Pattern Enumeration and Classification (CAPEC)

Are supplier employees trained to apply security design practices and kept aware of current weaknesses?

# Evaluate a Product's Threat Resistance

What product characteristics minimize opportunities to enter and change security characteristics?

- Exploitable features have been identified and eliminated where possible
- Design and coding weaknesses associated with exploitable features have been identified and mitigated (CWE)
- Independent validation and verification of threat resistance

Are supplier and acquirer product security responsibilities clearly assigned?

- Development and Integration
- Deployment and Operations

# Evaluate Maintaining Threat Resistance

Who assumes responsibility for preserving product's threat resistance after deployment and how is this monitored?

- Patching and version upgrades
- Changed usage patterns
- Expanded integration

How are usage changes identified and addressed?

- Change in feature usage or risks (new threats)
- Effects of supplier risk mitigations
- Effects of vendor upgrades/patches and local configuration changes
- Effects of integration into operations

# Effective Supply Chain Risk Management

Supply chain is well understood and documented

Available evidence indicates identified risks have been adequately reduced

For gaps in evidence, the impact of associated supply-chain risks has been evaluated and mitigation addressed.

# Control Points in a System Acquisition Lifecycle

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

# Findings from Pilot[1]

No widely accepted standards specifying “proper” security training of 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 requires 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 is used
- no formal acceptance criteria for assurance of COTS (commercial off-the-shelf) or code generated from COTS frameworks
- review is performed by Quality Control personnel with no security training

Focus is 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 completely 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 an acquirer 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 for supply chain acquisitions

# Contact Information


***Carol Woody***

(412) 268-9137

**cwoody@cert.org**


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

**http://www.cert.org/**

**http://www.sei.cmu.edu/**